Intel® Server Board M50CYP2SB Family

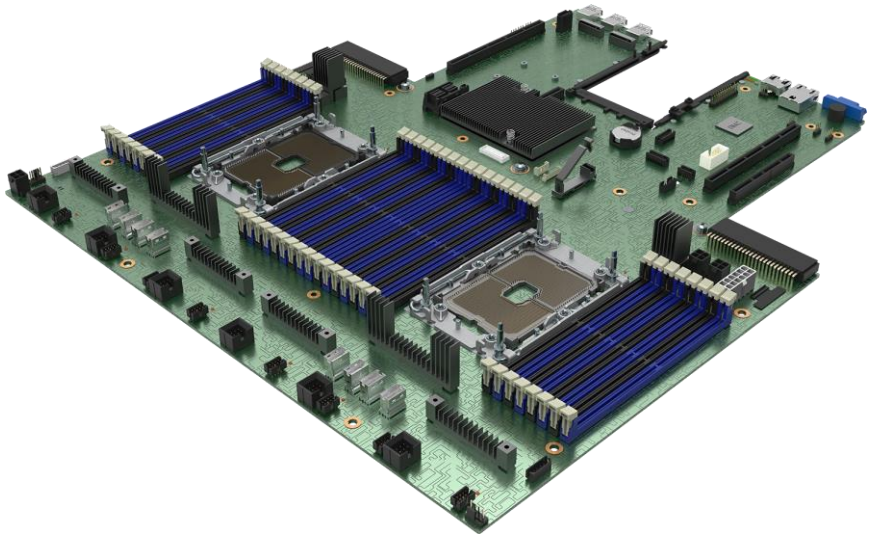
M50CYP2S

Technical Product Specification

An overview of product features, functions, architecture, and support specifications.

Rev. 1.0

May 2021



Delivering Breakthrough Data Center System Innovation – Experience What's Inside!

<This page intentionally left blank>

Document Revision History

Date	Revision	Changes
May 2021	1.0	Initial production release

Disclaimers

Intel technologies' features and benefits depend on system configuration and may require enabled hardware, software, or service activation. Performance varies depending on system configuration. No computer system can be absolutely secure. Check with your system manufacturer or retailer or learn more at intel.com.

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

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

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

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

This document contains information on products, services and/or processes in development. All information provided here is subject to change without notice. Contact your Intel representative to obtain the latest Intel product specifications.

Copies of documents which have an order number and are referenced in this document may be obtained by calling 1-800-548-4725 or by visiting www.intel.com/design/literature.htm.

Intel, Xeon, SpeedStep, Intel Optane, and the Intel logo are trademarks of Intel Corporation or its subsidiaries in the U.S. and/or other countries.

*Other names and brands may be claimed as the property of others.

Table of Contents

List of Figures

List of Tables

1. Introduction

This technical product specification (TPS) provides a high-level overview of the features, functions, architecture, and support specifications of the Intel® Server Board M50CYP2SB family.

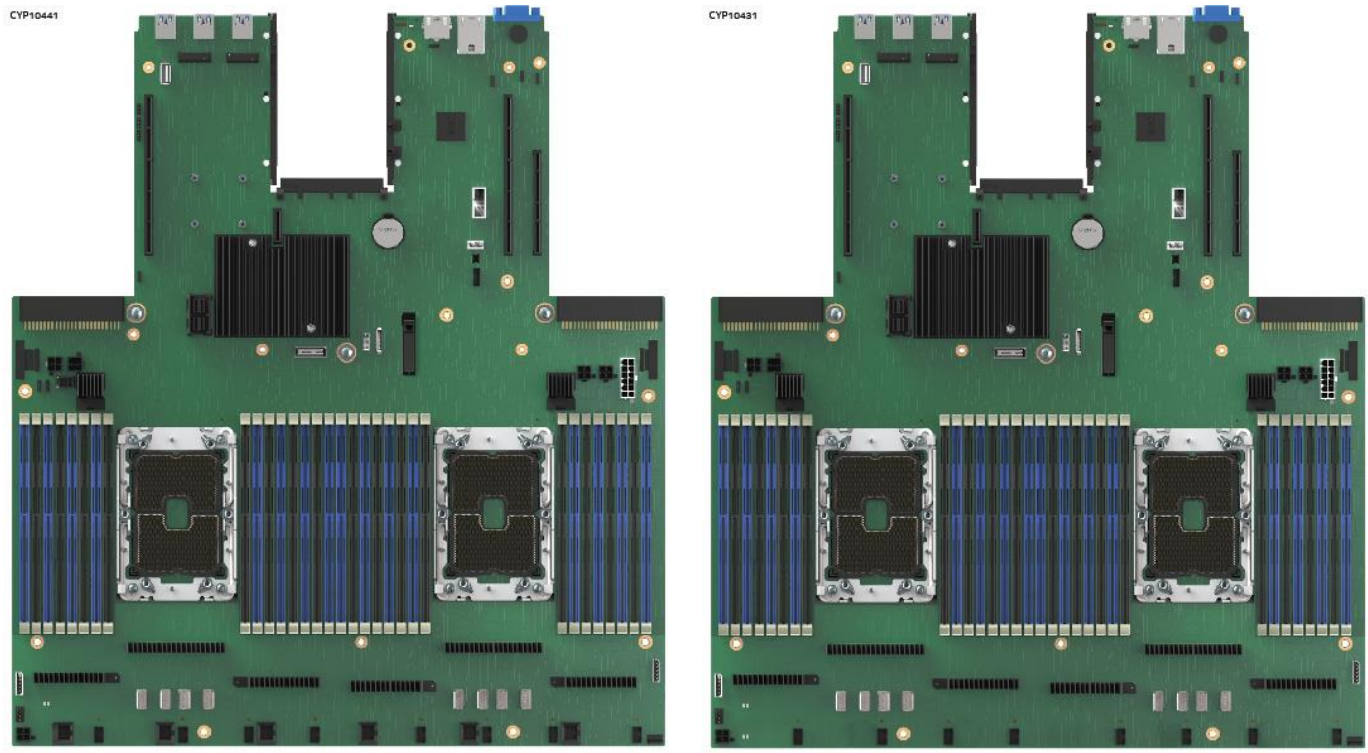
The Intel® Server Board M50CYP2SB family contains two server boards: M50CYP2SBSTD and M50CYP2SB1U. The boards are monolithic printed circuit board assemblies with features that are intended for high density rack mount server systems. These server boards are designed to support the 3rd Gen Intel® Xeon® Scalable processor family. Previous generation Intel® Xeon® processor and Intel® Xeon® Scalable processor families are not supported.

The Intel® Server Board M50CYP2SB family is a foundational building block of the server system. The family is backed by Intel design excellence, manufacturing expertise, and world-class support to deliver processing power with high levels of flexibility, manageability, and reliability.

Note: This document includes several references to Intel websites where additional product information can be downloaded. However, these public Intel sites do not include content for products in development. Content for these products will be available on the public Intel websites after their public launch.

Note: In this document, the 3rd Gen Intel® Xeon® Scalable processor family may be referred to simply as "processor".

Note: For more in-depth technical information, see the related documents in Section 1.1. Some of the documents listed in the appendix are classified as "Intel Confidential". These documents are made available under a Non-Disclosure Agreement (NDA) with Intel and must be ordered through your local Intel representative.



M50CYP2SBSTD Server Board M50CYP2SB1U Server Board

Figure 1. Intel® Server Board M50CYP2SB Family

1.1 Reference Documents

For additional information, see the product support collaterals specified in the following table. The following webpage provides support information for the M50CYP family:
https://www.intel.com/content/www/us/en/support/products/200321.html

Table 1. Intel® Server M50CYP Family Reference Documents and Support Collaterals

Topic	Document Title or Support Collateral	Document Classification
For system integration instructions and service guidance	*Intel® Server System M50CYP2UR Family System Integration and Service Guide*	Public
For system integration instructions and service guidance	*Intel® Server System M50CYP1UR Family System Integration and Service Guide*	Public
For technical system-level description	*Intel® Server System M50CYP2UR Family Technical Product Specification*	Public
For technical system-level description	*Intel® Server System M50CYP1UR Family Technical Product Specification*	Public
For technical board-level description	*Intel® Server Board M50CYP2SB Family Technical Product Specification*	Public
For server configuration guidance and compatibility	*Intel® Server M50CYP Family Configuration Guide*	Public
For information on the Integrated BMC Web Console	*Intel® Integrated Baseboard Management Controller Web Console (Integrated BMC Web Console) User Guide For the Intel® Server Board D50TNP and M50CYP Families*	Public
For BIOS technical information on Intel® Server M50CYP Family	*BIOS Firmware External Product Specification (EPS) For the Intel® Server Board D50TNP and M50CYP Families*	Intel Confidential
For BIOS setup information on Intel® Server M50CYP Family	*BIOS Setup Utility User Guide For the Intel® Server Board D50TNP and M50CYP Families*	Public
For BMC technical information on Intel® Server M50CYP Family	*Integrated Baseboard Management Controller Firmware External Product Specification For the Intel® Server System D50TNP and M50CYP Families*	Intel Confidential
Base specifications for the IPMI architecture and interfaces	*Intelligent Platform Management Interface Specification Second Generation v2.0*	Intel Confidential
Specifications for the PCIe* 3.0 architecture and interfaces	*PCIe* Base Specification, Revision 3.0* http://www.pcisig.com/specifications	Public
Specifications for the PCIe* 4.0 architecture and interfaces	*PCIe* Base Specification, Revision 4.0* http://www.pcisig.com/specifications	Public
Specification for OCP*	Open Compute Project* (OCP*) Specification	Intel Confidential
TPM for PC Client specifications	*TPM PC Client Specifications, Revision 2.0*	Intel Confidential
Functional specifications of 3rd Gen Intel® Xeon® Scalable processor family	*3rd Generation Intel® Xeon® Scalable Processors, Codename Ice Lake-SP External Design Specification (EDS):* Document IDs: 574451, 574942, 575291	Intel Confidential
BIOS and BMC Security Best Practices	*Intel® Server Systems Baseboard Management Controller (BMC) and BIOS Security Best Practices White Paper* https://www.intel.com/content/www/us/en/support/articles/000055785/server-products.html	Public
Managing an Intel Server Overview	*Managing an Intel Server System 2020* https://www.intel.com/content/www/us/en/support/articles/000057741/server-products.html	Public

Topic	Document Title or Support Collateral	Document Classification
For technical information on Intel® Optane™ persistent memory 200	*Intel® Optane™ Persistent Memory 200 Series Operations Guide*	Intel Confidential
For setup information for Intel® Optane™ persistent memory 200	*Intel® Optane™ Persistent Memory Startup Guide*	Public
For latest system software updates: BIOS and Firmware	*Intel® System Update Package (SUP) for Intel® Server M50CYP Family*	Public
	Intel® System Firmware Update Utility (SYSFWUPDT) - Various operating system support	
	Intel® System Firmware Update Utility User Guide	
To obtain full system information	*Intel® SYSINFO Utility for Intel® Server M50CYP Family*	Public
	Intel® System Information Utility User Guide	
To configure, save, and restore various system options	*Intel® SYSCFG Utility for Intel® Server M50CYP Family – Various operating system support*	Public
	Intel® System Configuration Utility User Guide	
Product Warranty Information	*Warranty Terms and Conditions* https://www.intel.com/content/www/us/en/support/services/000005886.html	Public

Note: Intel Confidential documents are made available under a Non-Disclosure Agreement (NDA) with Intel and must be ordered through your local Intel representative.

2. Server Board Family Overview

This chapter identifies the board's features and functions, provides mechanical dimensional diagrams, and an overview of each board architecture.

2.1 Server Board Feature Set

The following table provides a high-level overview of the Intel® Server Board M50CYP2SB family.

Table 2. Intel® Server Board M50CYP2SB Family Features

Feature	Details
Server Board	• Intel® Server Board M50CYP2SBSTD and Intel® Server Board M50CYP2SB1U
Server Board Dimensions	• 477.36 mm length x 427.98 mm width x 1.93 mm thickness

Processor Support	• Dual Socket-P4 LGA4189
	• Supported 3rd Gen Intel® Xeon® Scalable processor family SKUs:
	  ○ Intel® Xeon® Platinum 8300 processor
	  ○ Intel® Xeon® Gold 6300 processor
	  ○ Intel® Xeon® Gold 5300 processor
	  ○ Intel® Xeon® Silver 4300 processor
	Note: Supported 3rd Gen Intel® Xeon® Scalable processor SKUs must Not end in (H), (L), (U), or (Q). All other processor SKUs are supported.
	• UPI links: up to three at 11.2 GT/s (Platinum and Gold families) or up to two at 10.4 GT/s (Silver family)
	Note: Previous generation Intel® Xeon® processors are not supported.

Maximum Supported Processor Thermal Design Power (TDP)	• 3rd Gen Intel® Xeon® Scalable processors can operate up to 270 W. **Note:** The maximum supported processor TDP depends on system configuration.
Chipset	• Intel® C621A Series Chipset

Memory Support	• 32 DIMM slots
	  ○ 16 DIMM slots per processor, eight memory channels per processor
	  ○ Two DIMMs per channel
	• All DDR4 DIMMs must support ECC
	• Registered DDR4 (RDIMM), 3DS-RDIMM, Load Reduced DDR4 (LRDIMM), 3DS-LRDIMM
	Note: 3DS = 3 Dimensional Stacking
	• Intel® Optane™ persistent memory 200 series
	• Memory capacity
	  ○ Up to 6 TB per processor (processor SKU dependent)
	• Memory data transfer rates
	  ○ Up to 3200 MT/s at one or two DIMMs per channel (processor SKU dependent)
	• DDR4 standard voltage of 1.2V

System Fan Support	• Six 6-pin fan connectors (**Intel® Server Board M50CYP2SBSTD**) • Eight 8-pin fan connectors (**Intel® Server Board M50CYP2SB1U and M50CYP2SBSTD**) • CPU fan headers (one for each CPU)
Onboard Network Support	Provided by optional Open Compute Project (OCP*) module support. See below.
Open Compute Project* (OCP*) Module Support	Onboard x16 PCIe* 4.0 OCP 3.0 Mezzanine connector (Small Form-Factor) slot supports the following Intel accessory options: • Dual port, RJ45, 10/1 GbE, - iPC – X710T2LOCPV3 • Quad port, SFP+ DA, 4x 10 GbE – iPC- X710DA4OCPV3 • Dual Port, QSFP28 100/50/25/10 GbE – iPC- E810CQDA2OCPV3 • Dual Port, SFP28 25/10 GbE – iPC – E810XXVDA2OCPV3

Feature	Details
Riser Card Support	Concurrent support for up to three riser cards with support for up to eight PCIe* add-in cards. In the below description FH = Full Height, FL = Full Length, HL =Half Length, LP = Low Profile. **Riser Slot #1:** • Riser Slot #1 supports x32 PCIe* lanes, routed from CPU 0 • PCIe* 4.0 support for up to 64 GB/s **Riser Slot #1 supports the following Intel Riser Card options:** • Two PCIe* slot riser card supporting (one) - FH/FL double-width slot (x16 electrical, x16 mechanical) + (one) - FH/HL single-width slot (x16 electrical, x16 mechanical) iPC – CYP2URISER1DBL • Three PCIe* slot riser card supporting (one) - FH/FL single-width slot (x16 electrical, x16 mechanical) + (one) - FH/FL single-width slot (x8 electrical, x16 mechanical) + (one) - FH/HL single-width slot (x8 electrical, x8 mechanical) iPC – CYP2URISER1STD • NVMe* riser card supporting (one) – HL or FL single-width slot (x16 electrical, x16 mechanical) + (two) - x8 PCIe* NVMe* SlimSAS* connectors, each with a re-timer. iPC – CYP2URISER1RTM • One PCIe* slot Riser card supporting (one) – LP/HL, single-width slot (x16 electrical, x16 mechanical) iPC – CYP1URISER1STD **Riser Slot #2:** • Riser Slot #2 supports x32 PCIe* lanes, routed from CPU 1 • PCIe* 4.0 support for up to 64 GB/s **Riser Slot #2 supports the following Intel Riser Card options:** • Two PCIe* slot riser card supporting (one) - FH/FL double-width slot (x16 electrical, x16 mechanical) + (one) - FH/HL single-width slot (x16 electrical, x16 mechanical) iPC – CYP2URISER2DBL • Three PCIe* slot riser card supporting (one) - FH/FL single-width slot (x16 electrical, x16 mechanical) + (one) - FH/FL single-width slot (x8 electrical, x16 mechanical) + (one) FH/HL single-width slot (x8 electrical, x8 mechanical) iPC – CYP2URISER2STD • One PCIe* slot Riser card supporting (one) – LP/HL, single-width slot (x16 electrical, x16 mechanical) iPC – CYP1URISER2STD • NVMe* Riser card supporting (one) – LP/HL, single-width slot (x16 electrical, x16 mechanical) + (one) - x8 PCIe* NVMe* SlimSAS* connector with re-timer. iPC – CYP1URISER2KIT **PCIe* Interposer Riser Slot** • Interposer riser card supports x8 PCIe* lanes, route from CPU 1 • PCIe* 4.0 support for 32 GB/s • PCIe* Interposer Riser Slot supports the Intel interposer riser card as an accessory option. This card supports one PCIe* add-in card (x8 electrical, x8 mechanical). The PCIe* interposer riser card can be used only when it is connected to the PCIe* NVMe* riser card in Riser Slot #2 (iPC – CYP1URISER2KIT). The interposer card uses x8 PCIe* data lanes signals routed from the PCIe* SlimSAS* connector on the PCIe* NVMe* riser card. The Intel accessory kit includes the PCIe* interposer riser card, PCIe* NVMe* riser card, and PCIe* interposer cable. iPC – CYP1URISER2KIT **Riser Slot #3:** • Riser Slot #3 supports x16 PCIe* lanes, route from CPU 1 • PCIe* 4.0 support for up to 32 GB/s **Riser Slot #3 supports the following Intel Riser Card options:** • Two PCIe* slot riser card supporting (two) LP/HL single-width slots (x16 mechanical, x8 electrical) iPC – CYP2URISER3STD • NVMe* riser card supporting (two) – PCIe* NVMe* SlimSAS* connectors with re-timers iPC – CYPRISER3RTM

PCIe* NVMe* Support	• Support for up to 10 PCIe* NVMe* Interconnects
	  ○ Eight onboard SlimSAS* connectors, four per processor
	  ○ Two M.2 NVMe/SATA connectors
	• Additional NVMe* support through select Riser Card options (See Riser Card Support)
	• Intel® Volume Management Device (Intel® VMD) 2.0 support
	• Intel® Virtual RAID on CPU 7.5 (Intel® VROC 7.5) support using one of the three types of VROC keys (available as an Intel accessory option)

Feature	Details
Video Support	• Integrated 2D video controller • 128 MB of DDR4 video memory • One VGA DB-15 external connector in the back

Onboard SATA Support	• 10 x SATA III ports (6 Gb/s, 3 Gb/s and 1.5 Gb/s transfer rates supported)
	  ○ Two M.2 connectors – SATA / PCIe*
	  ○ Two 4-port Mini-SAS HD (SFF-8643) connectors

USB Support	• Three external USB 3.0 connectors intended for rear of chassis use. • Internal 26-pin connector for optional one USB 3.0 port and one USB 2.0 port front panel support • One USB 2.0 internal Type-A header
Serial Support	• One external RJ-45 serial-A port connector on the back • One internal DH-10 serial-B port header for optional front or rear serial port support. The port follows DTK pinout specifications.
Server Management	• Integrated Baseboard Management Controller (BMC) • Intelligent Platform Management Interface (IPMI) 2.0 compliant • Support for Intel® Data Center Manager (DCM) • Support for Intel® Server Debug and Provisioning Tool (SDPTool) • Redfish* compliant • Support for Intel Server Management Software • Dedicated onboard RJ45 1 GbE management port • Light Guided Diagnostics
System Configuration and Recovery Jumpers	• BIOS load defaults • BIOS Password clear • Intel® Management Engine firmware force update Jumper • BMC force update • BIOS_SVN Downgrade • BMC_SVN Downgrade For more information, see Chapter 13.
Security Support	• Intel® Platform Firmware Resilience (Intel® PFR) technology with an I^2C interface • Intel® Software Guard Extensions (Intel® SGX) • Intel® CBnT – Converged Intel® Boot Guard and Trusted Execution Technology (Intel® TXT) • Intel® Total Memory Encryption (Intel® TME) • Trusted platform module 2.0 (Rest of World) – iPC J33567-151 (accessory option) • Trusted platform module 2.0 (China Version) – iPC J12350-150 (accessory option)
BIOS	Unified Extensible Firmware Interface (UEFI)-based BIOS (legacy boot not supported)

2.2 Server Board Component / Feature Identification

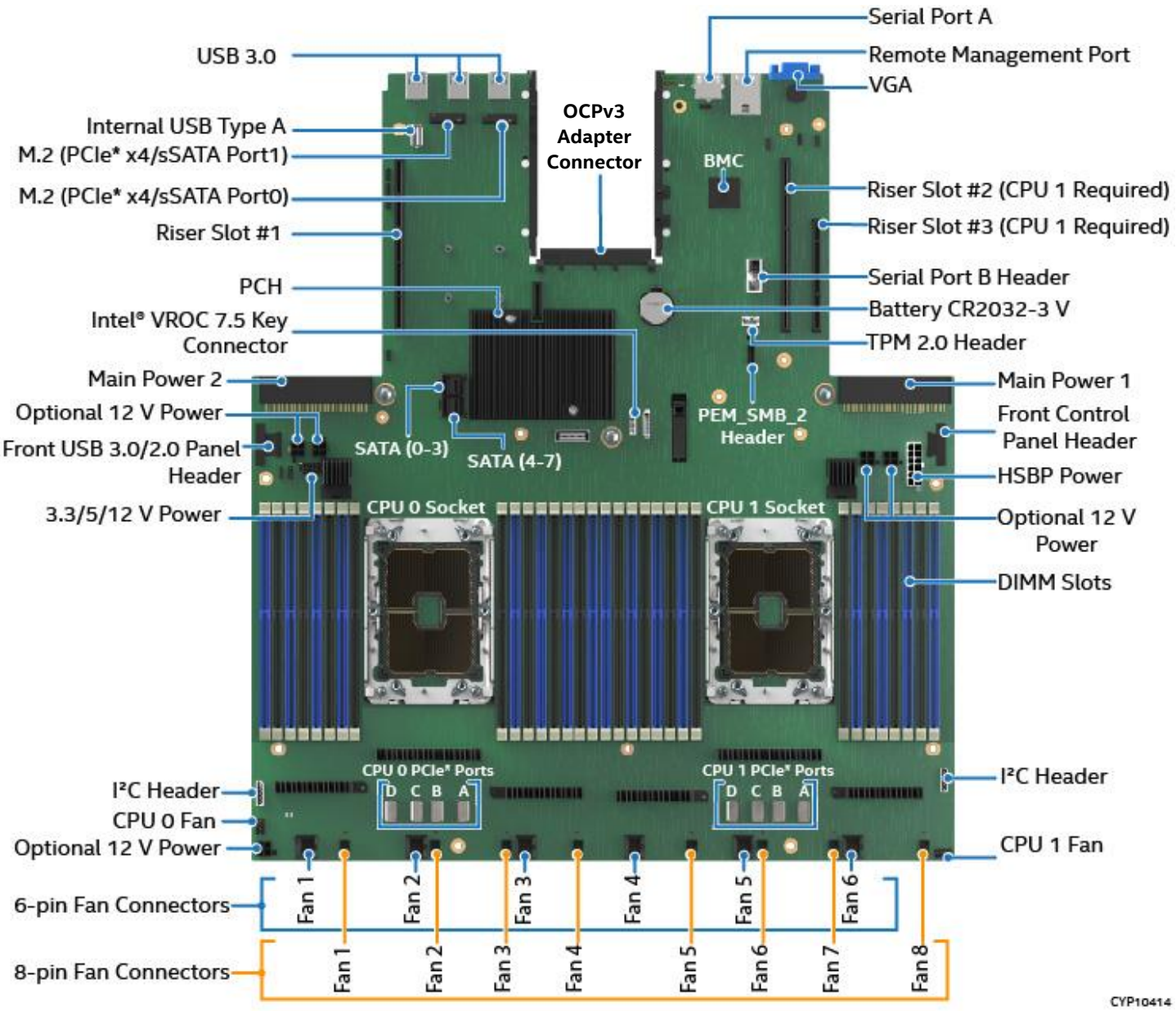


Figure 2. Intel® Server Board M50CYP2SBSTD Component / Feature Identification

Note: The features identified in the above figure represent their intended usage when the board is integrated into an Intel chassis.

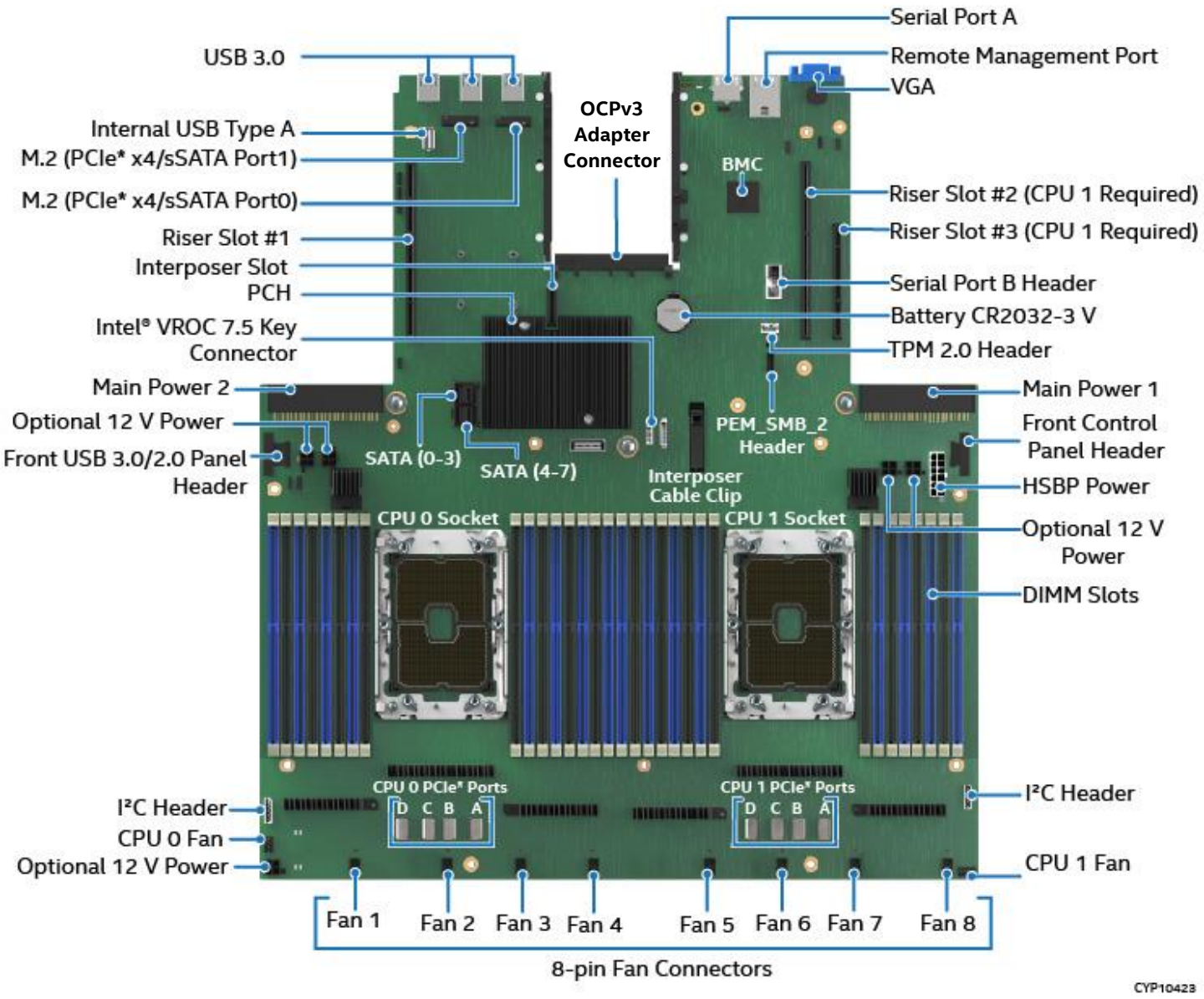


Figure 3. Intel® Server Board M50CYP2SB1U Component / Feature Identification

Note: The features identified in the above figure represent their intended usage when the board is integrated into an Intel chassis.

The server board includes LEDs to identify system status and/or indicate a component fault.

The following figures identify Light Guided Diagnostic LEDs on the server board. For more information on Intel® Light-Guided Diagnostics, see Chapter 10.

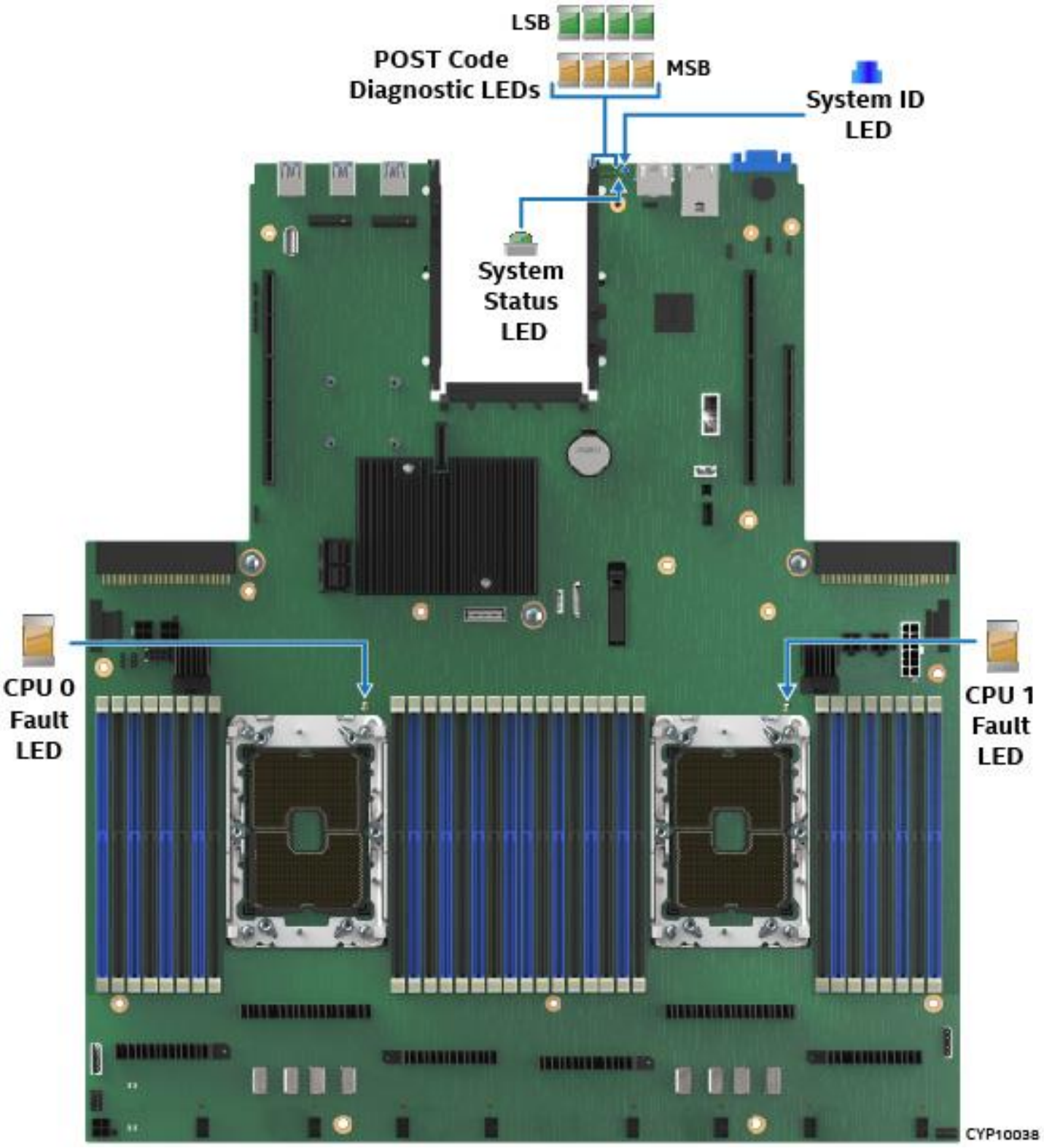


Figure 4. Intel® Light-Guided Diagnostics – LED Identification

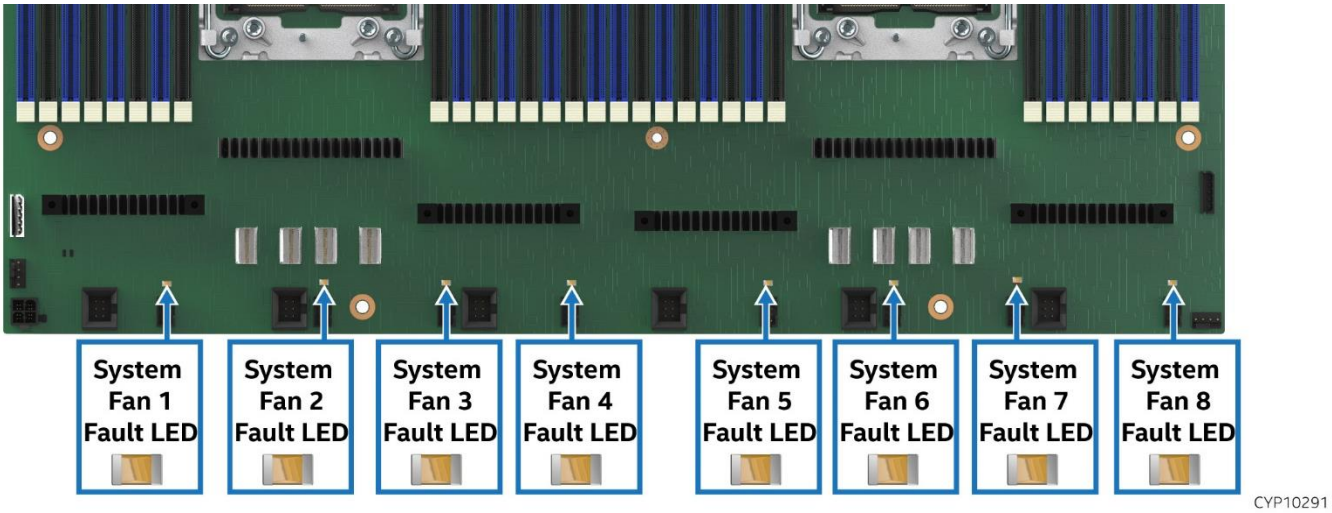


Figure 5. Fan fault LEDs on Intel® Server Board M50CYP2SB1U

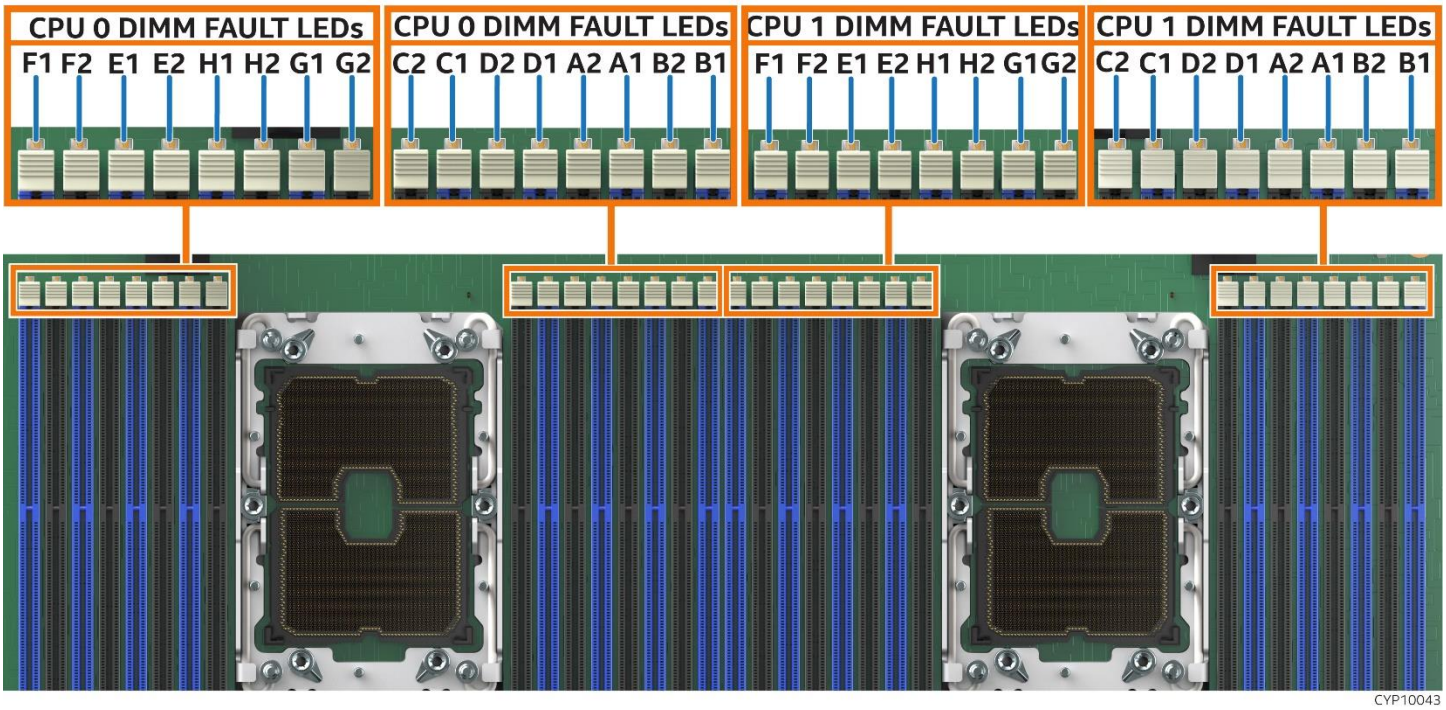


Figure 6. Intel® Light-Guided Diagnostics - DIMM Fault LEDs

The server board includes several jumper headers (see Figure 7) that can be used to configure, protect, or recover specific features of the server board. For more information on reset and recovery jumpers, see Chapter 13.

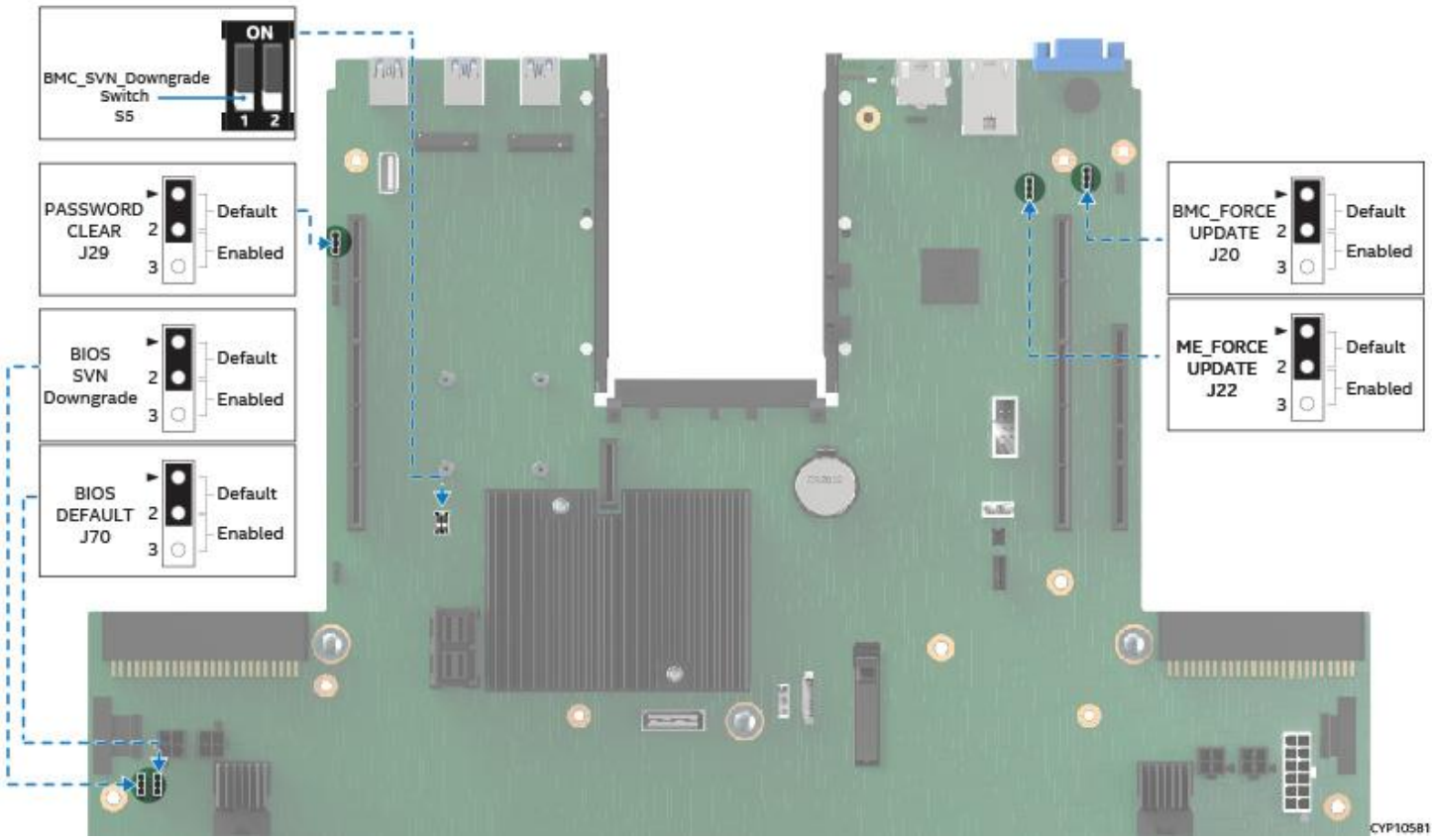


Figure 7. System Configuration and Recovery Jumpers

2.3 Server Board Dimensions

The following figure shows the Intel® Server Board M50CYP2SBSTD and M50CYP2SB1U dimensions.

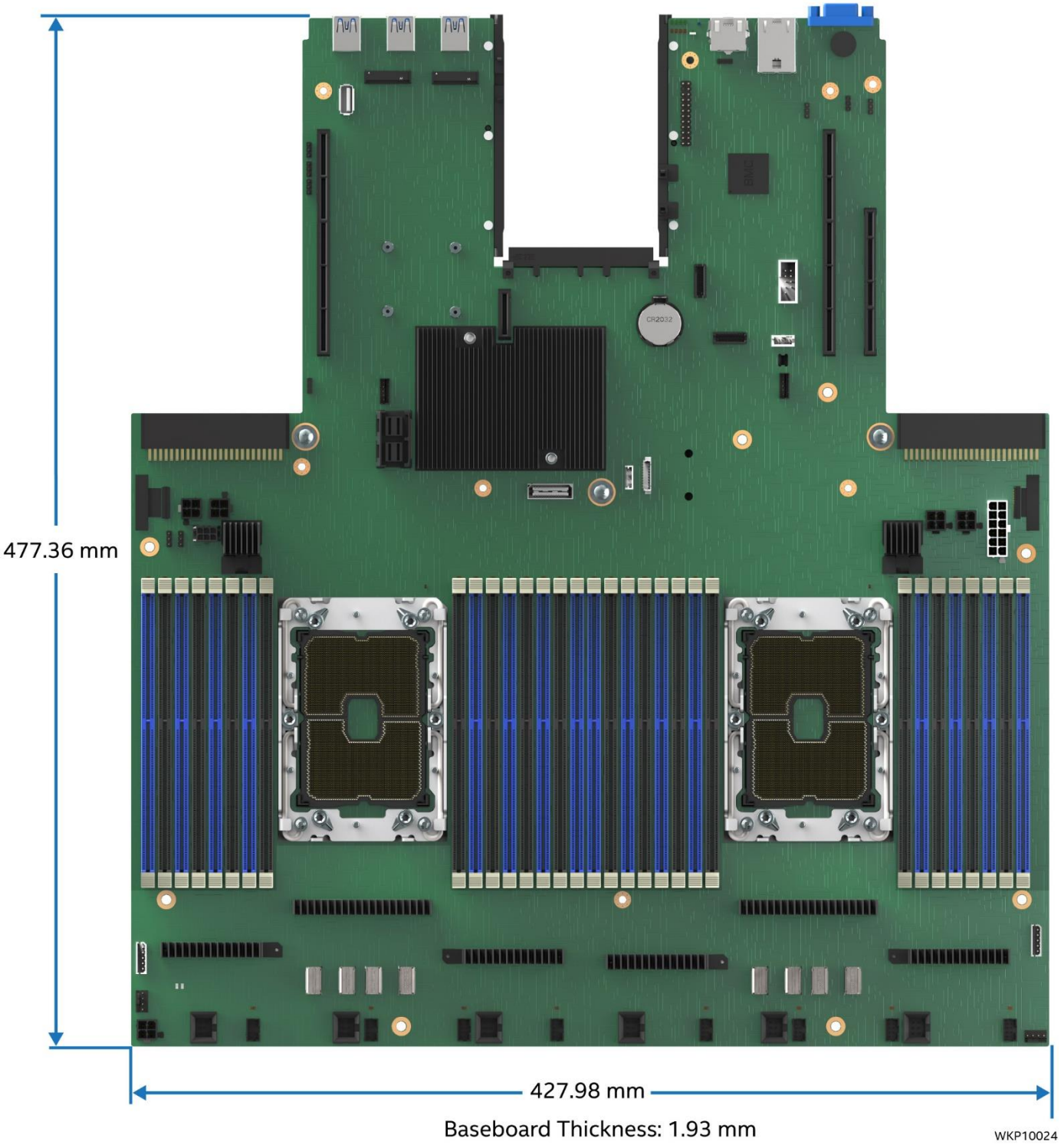


Figure 8. Intel® Server Board M50CYP2SBSTD and M50CYP2SB1U Board Dimensions

2.4 Server Board Mechanical Drawings

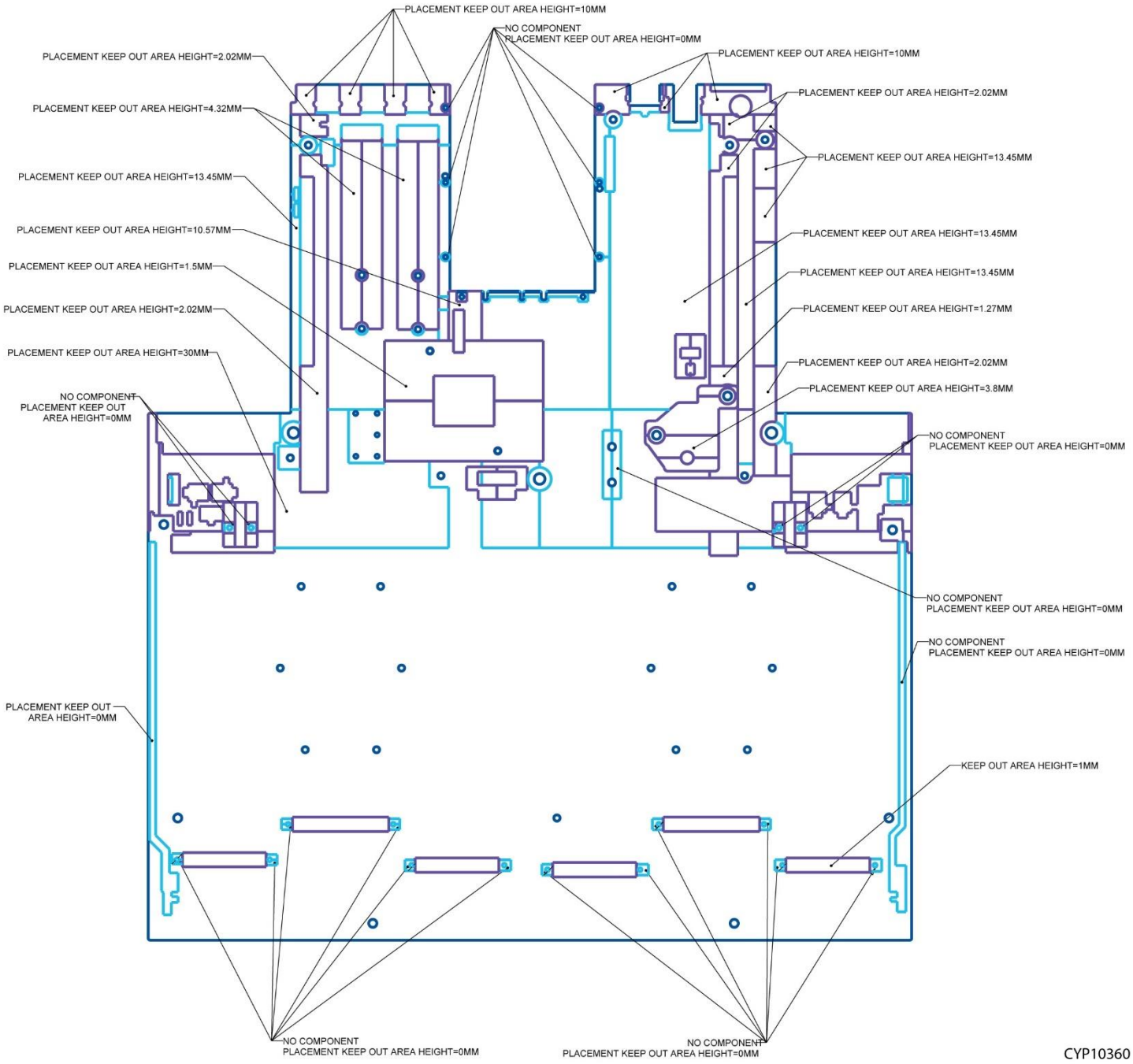


Figure 9. Intel® Server Board M50CYP2SB Family Top Surfaces Keep Out Zone (drawing 1)

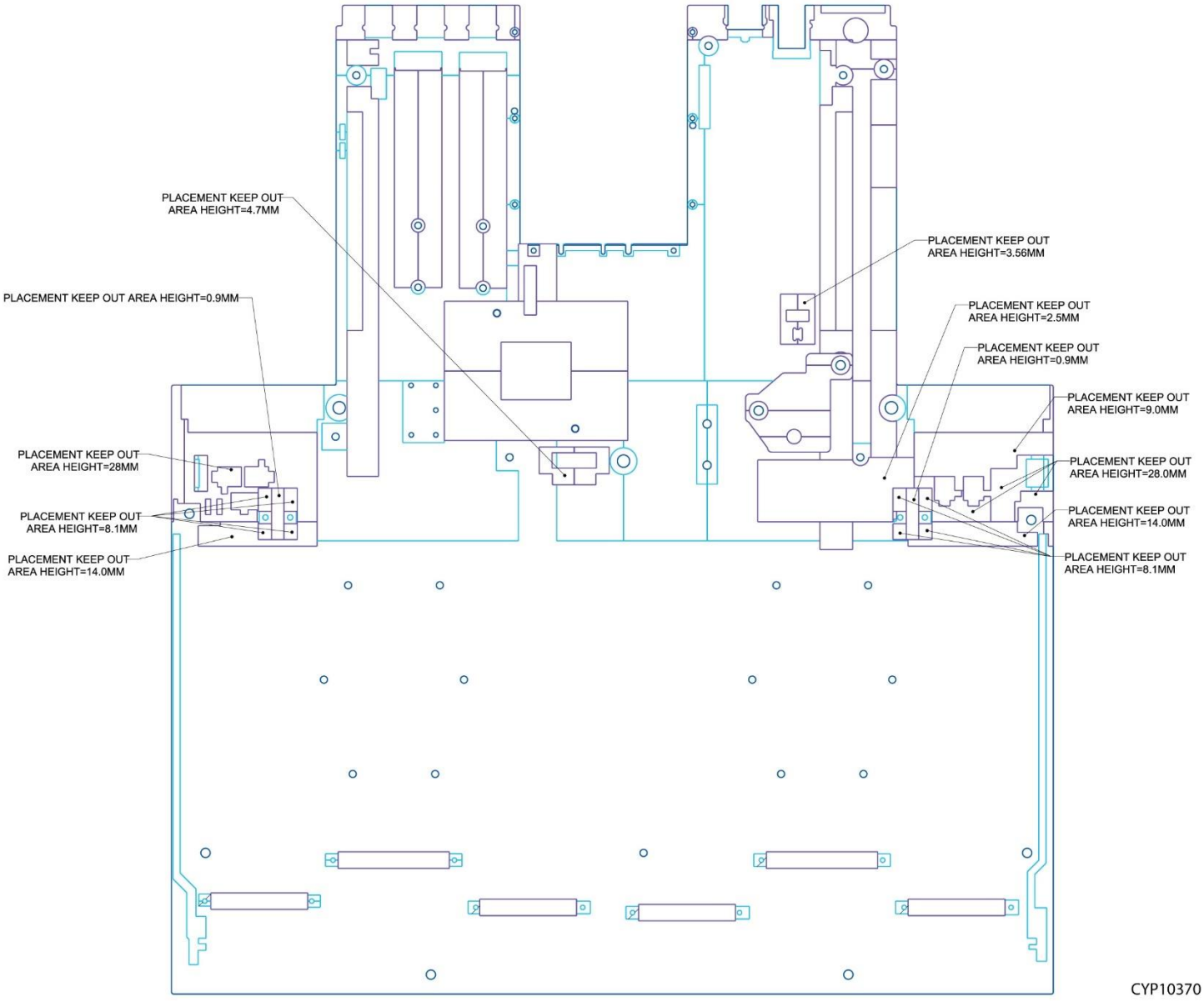


Figure 10. Intel® Server Board M50CYP2SB Family Top Surface Keep Out Zone (drawing 2)

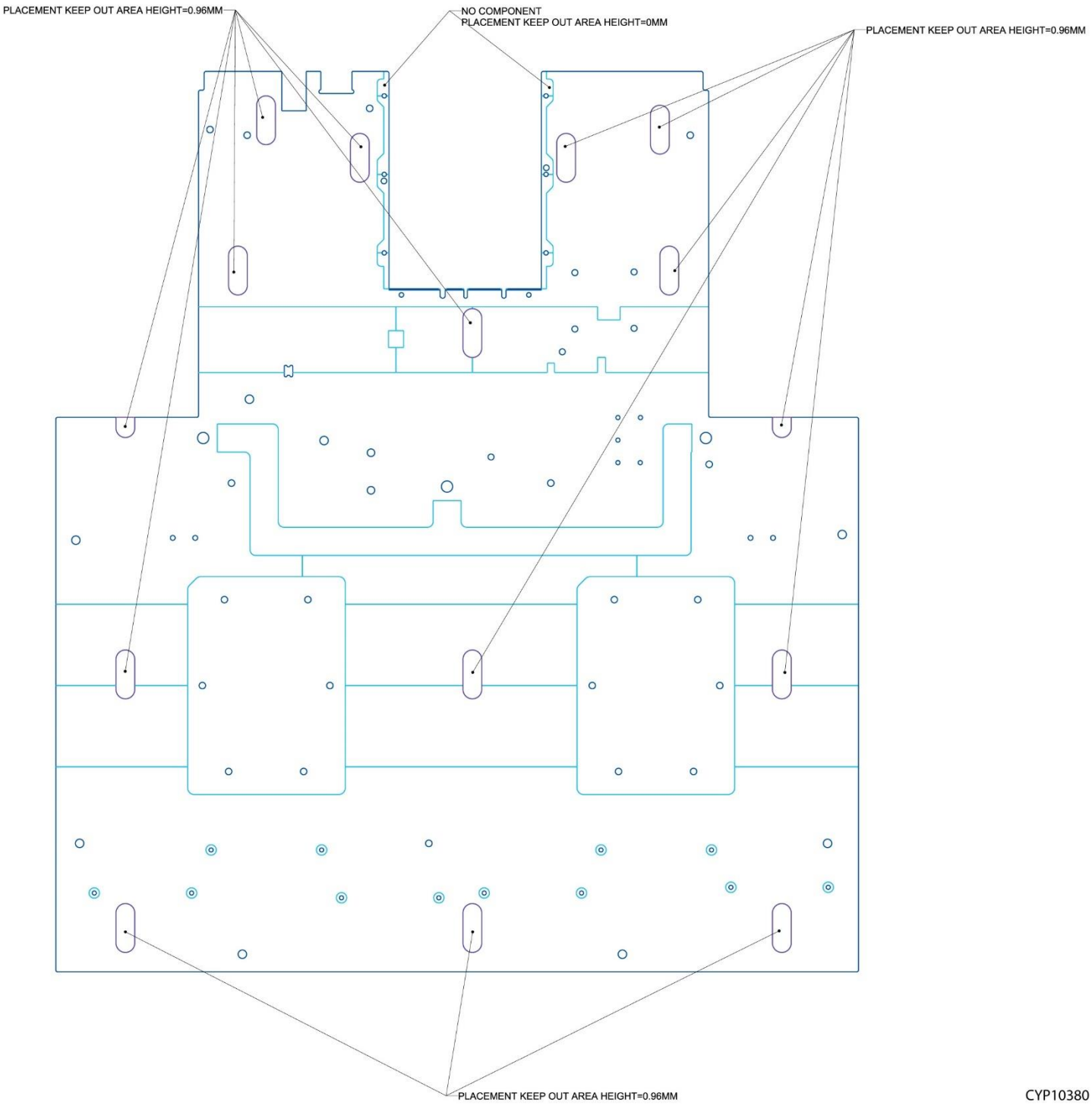


Figure 11. Intel® Server Board M50CYP2SB Family Bottom Surface Keep Out Zone (drawing 1)

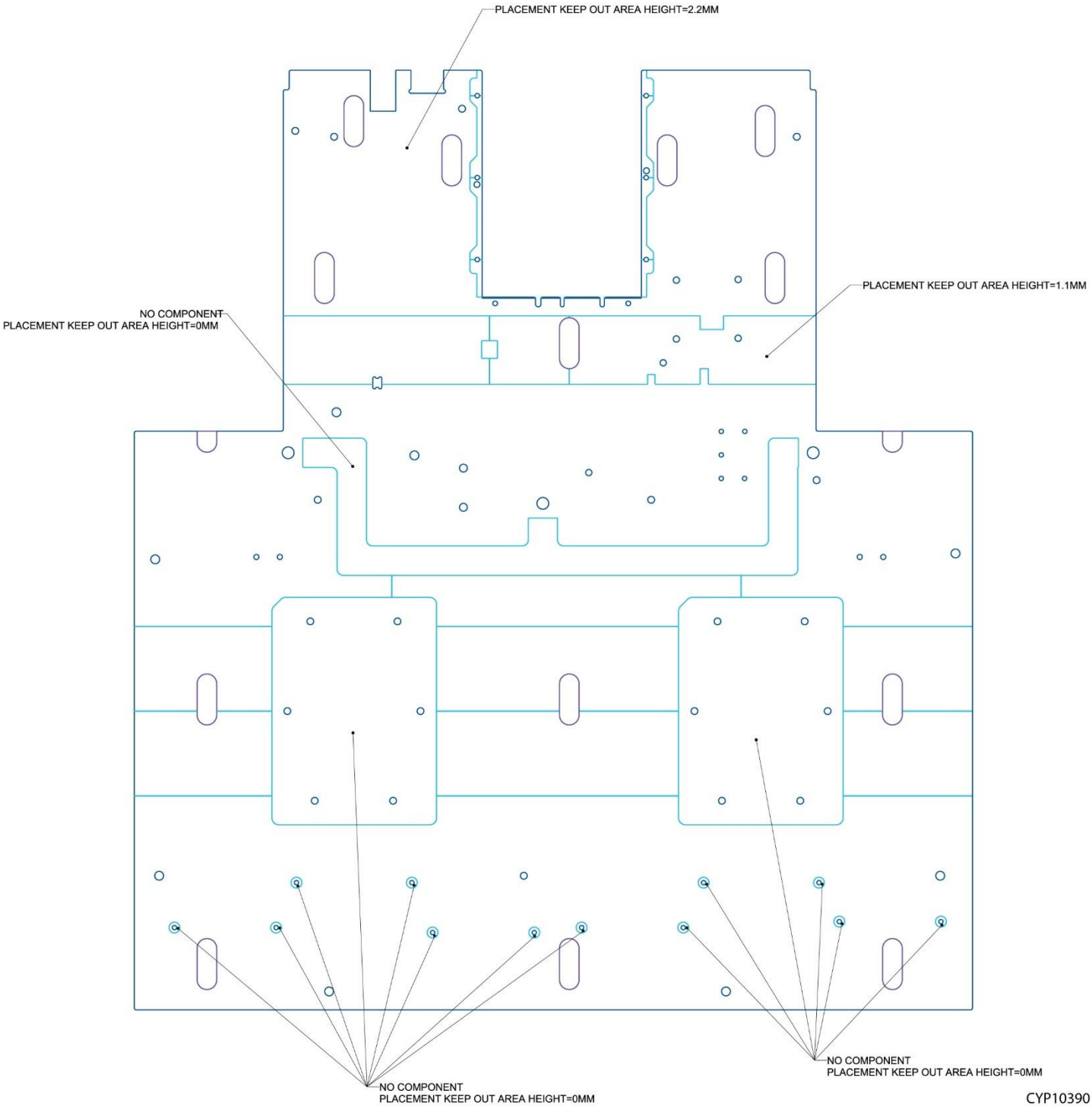


Figure 12. Intel® Server Board M50CYP2SB Family Bottom Surface Keep Out Zone (drawing 2)

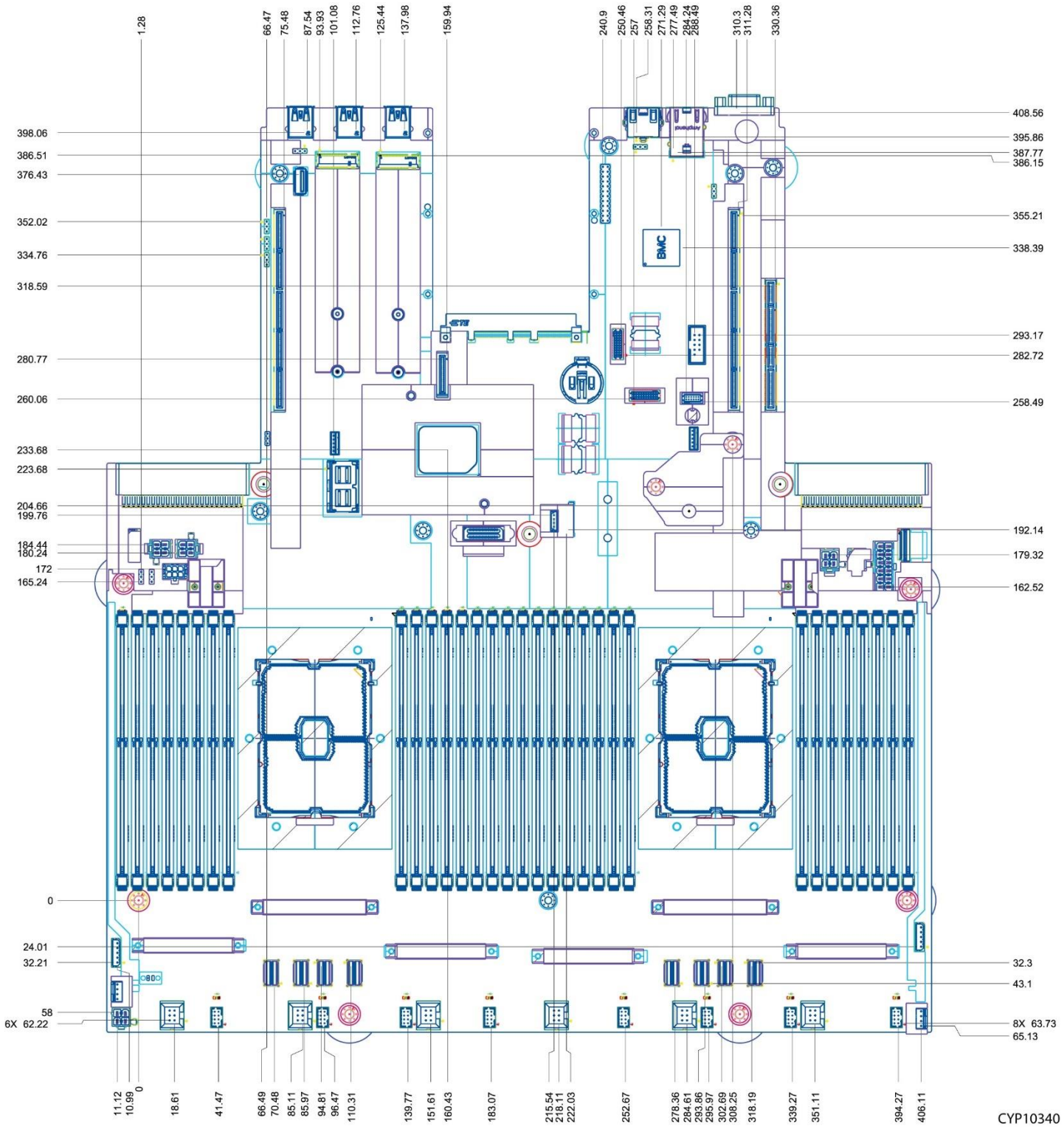


Figure 13. Intel® Server Board M50CYP2SB Family Components Position (drawing 1)

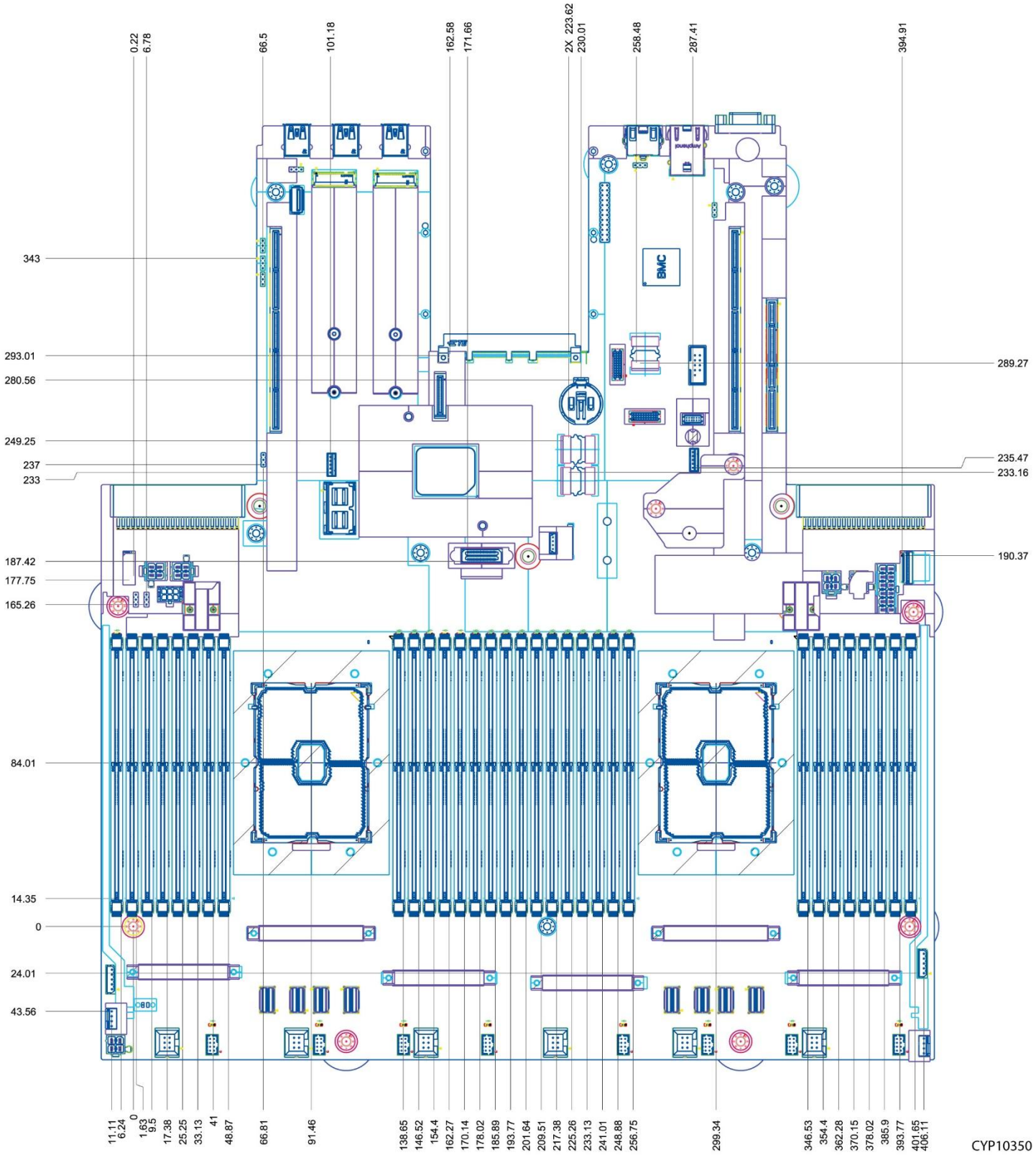


Figure 14. Intel® Server Board M50CYP2SB Family Components Position (drawing 2)

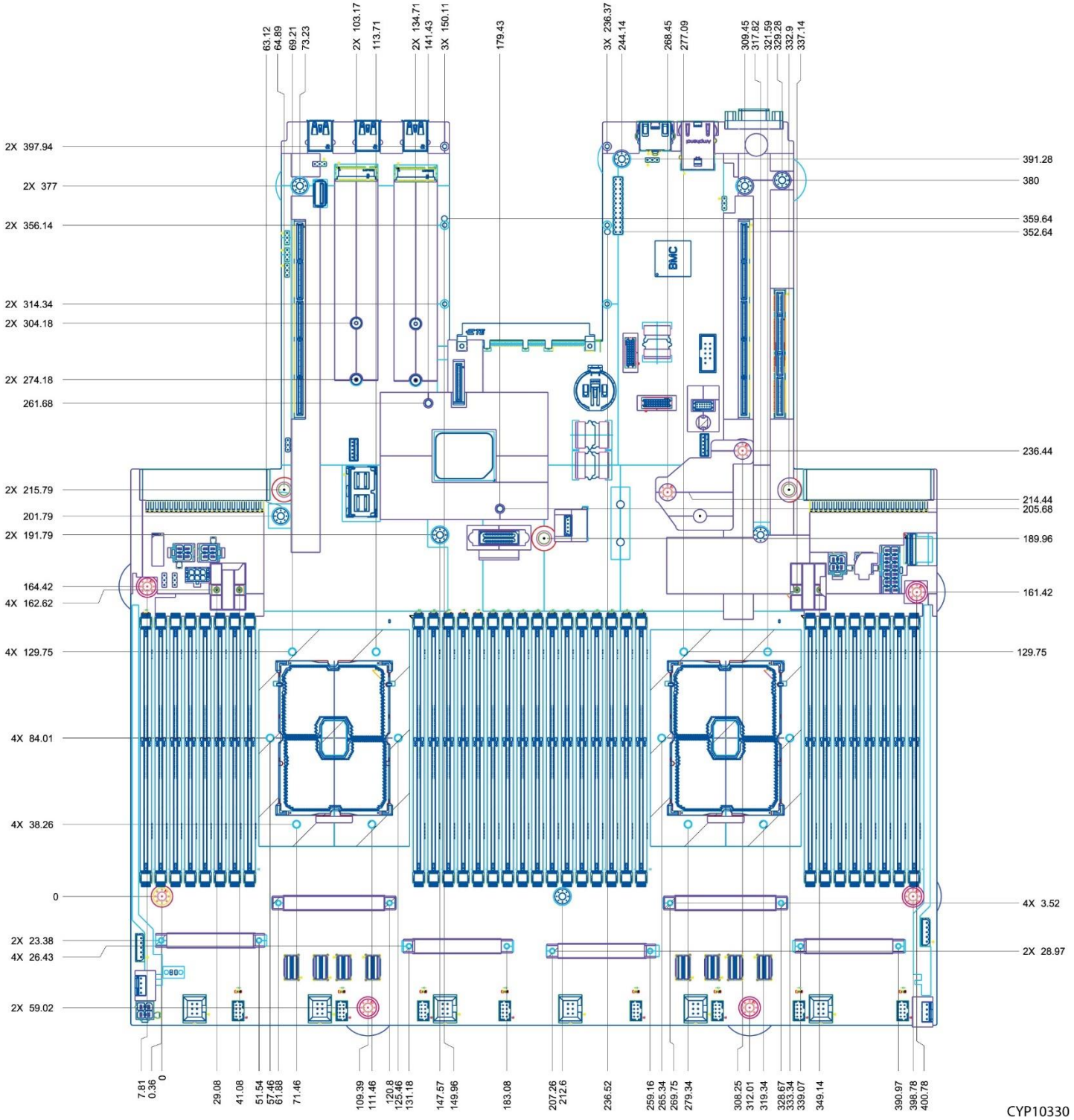


Figure 15. Intel® Server Board M50CYP2SB Family Holes Position

2.5 Server Board Architecture Overview

The architecture of the Intel® Server Board M50CYP2SB family was developed around the integrated features and functions of the 3rd Gen Intel® Xeon® Scalable processor family, Intel® C621A chipset (PCH), and ASPEED* AST2500 baseboard management controller (BMC).

The following figure provides an overview of the Intel® Server Board M50CYP2SBSTD architecture, showing the features and interconnects of the major subsystem components. Figure 2 provides a general overview of the physical server board, identifying key feature and component locations.

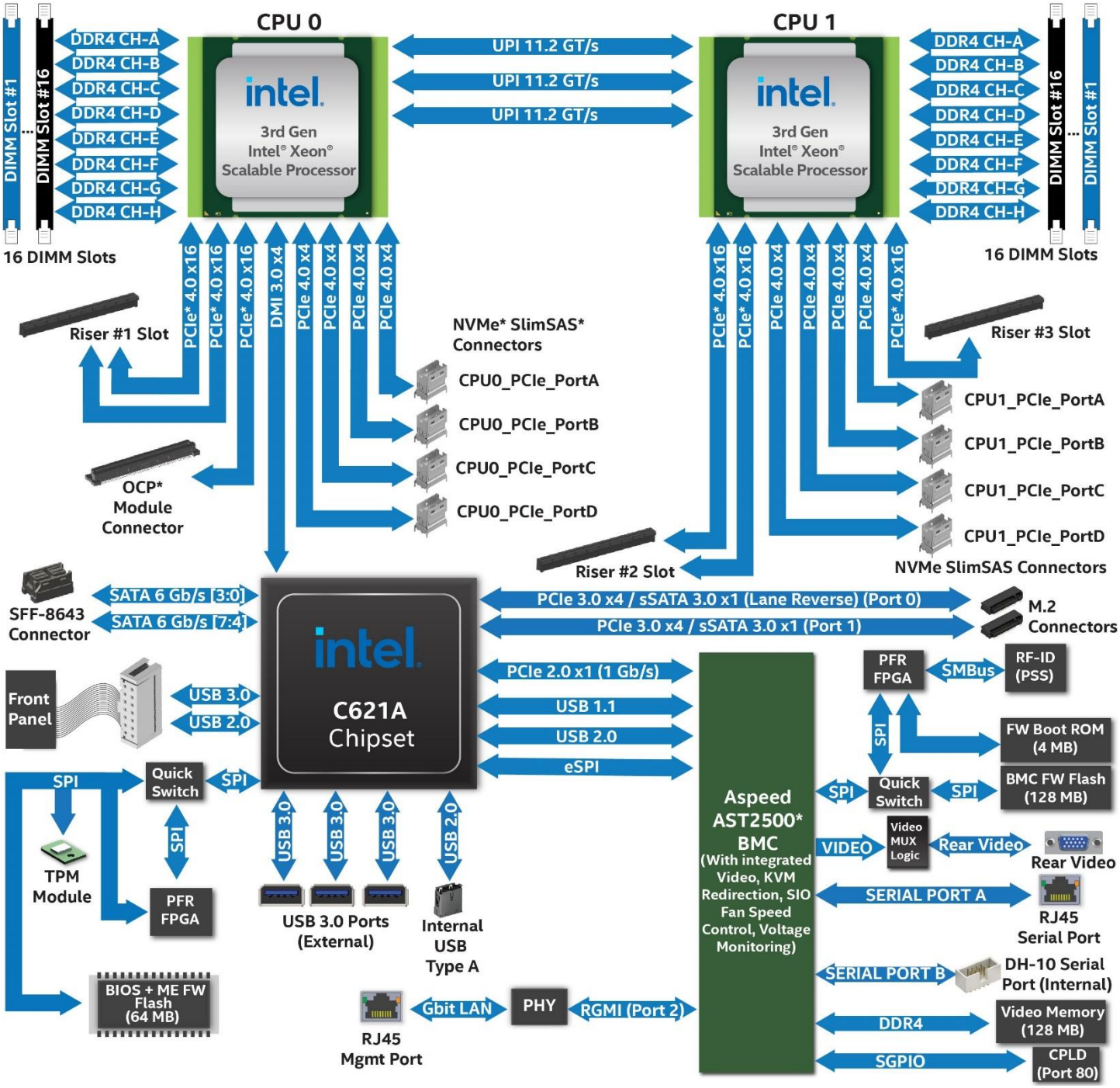


Figure 16. Intel® Server Board M50CYP2SBSTD Architectural Block Diagram

The following figure provides an overview of the Intel® Server Board M50CYP2SB1U architecture, showing the features and interconnects of the major subsystem components. Figure 3 provides a general overview of the physical server board, identifying key feature and component locations.

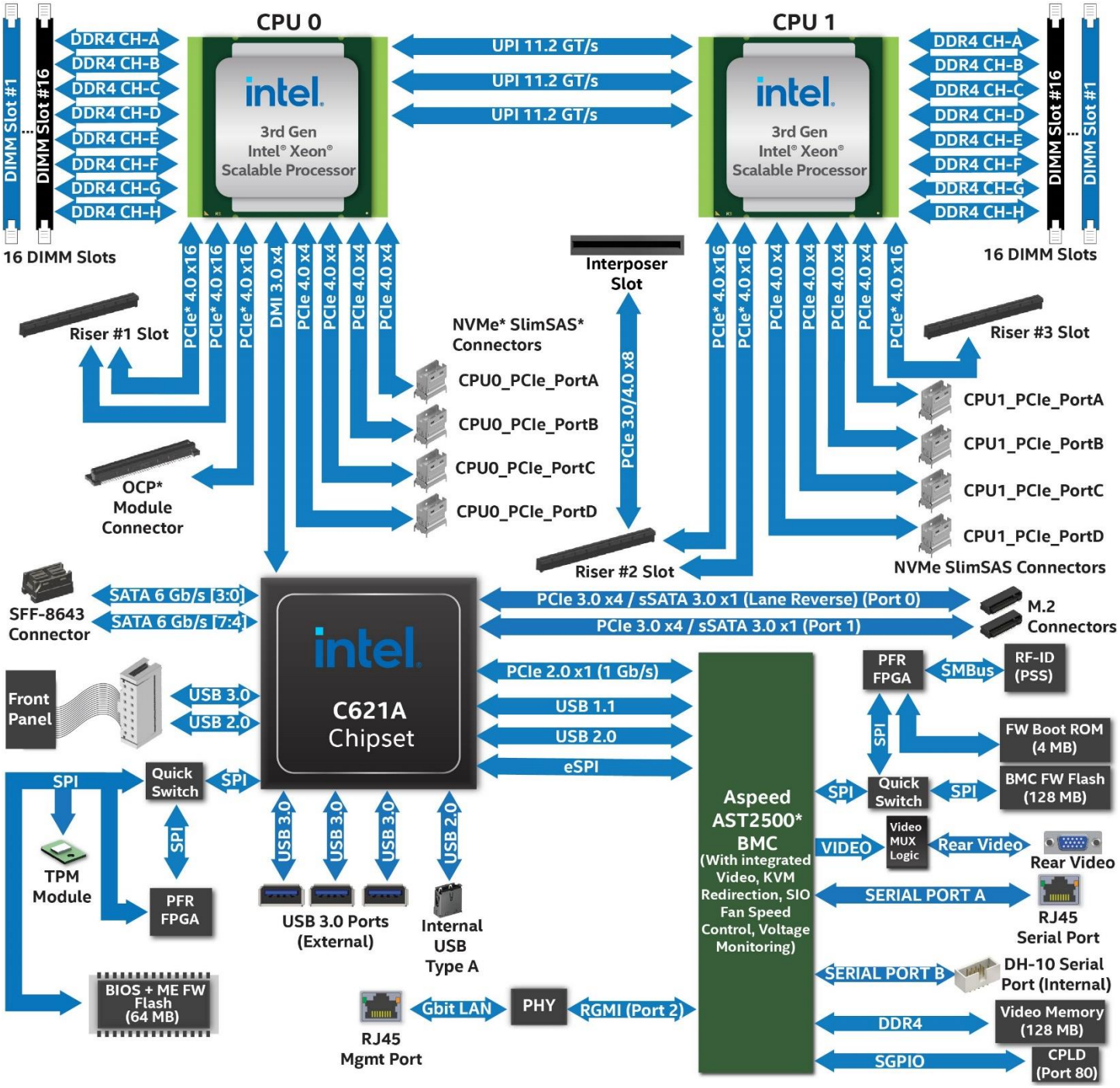


Figure 17. Intel® Server Board M50CYP2SB1U Architectural Block Diagram

3. Processor Support

The server board includes two Socket-P4 LGA4189 processor sockets compatible with the 3rd Gen Intel® Xeon® Scalable processor family. The server board supports the processor family with a maximum TDP of 270 W.

Note: Thermal Design Power (TDP) support may vary depending on the cooling capabilities of the chosen server chassis. Check the server chassis or server system product specifications to determine maximum supported processor TDP.

Note: Previous generations Intel® Xeon® processor and Intel® Xeon® Scalable processor families and their supported processor heat sinks are not compatible on server boards described in this document.

3.1 Processor Heat Sink Module (PHM) Assembly and Processor Socket Assembly

A processor heat sink module (PHM) assembly and processor socket assembly (also called "loading mechanism") are necessary to install a processor to the server board. The following figure identifies each component associated with the PHM and processor socket assembly.

Note: The following figure identifies the PHM components, not the processor installation process.

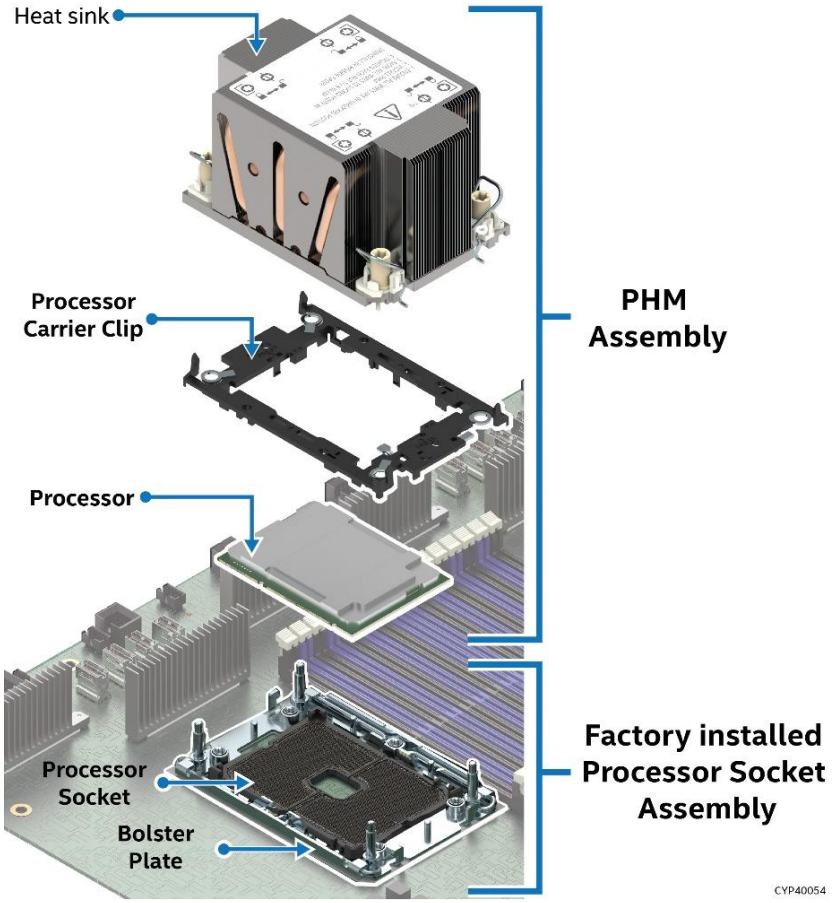


Figure 18. PHM Components and Processor Socket Reference Diagram

3.2 Processor Thermal Design Power (TDP) Support

To allow optimal operation and long-term reliability, the processor must remain within the defined minimum and maximum case temperature (T_{CASE}) specifications. Thermal solutions not designed to provide sufficient thermal capability may affect the long-term reliability of the processor and system. The server board described in this document is designed to support the 3rd Gen Intel® Xeon® Scalable processor family TDP guidelines up to and including 270 W.

Disclaimer Note: Intel® server boards contain several high-density VLSI and power delivery components that need adequate airflow to cool. Intel ensures through its own chassis development and testing that when Intel® server building blocks are used together; the fully integrated system meets the intended thermal requirements of these components. It is the responsibility of the system integrator who chooses not to use Intel-developed server building blocks to consult vendor datasheets and operating parameters to determine the amount of airflow required for the specific application and environmental conditions. Intel cannot be held responsible if components fail or the server board does not operate correctly when used outside any of its published operating or non-operating limits.

3.3 Processor Family Overview

The Intel® Server Board M50CYP2SB family supports the 3rd Gen Intel® Xeon® Scalable processor family. Processor shelves within the product family are identified as shown in the following figure.

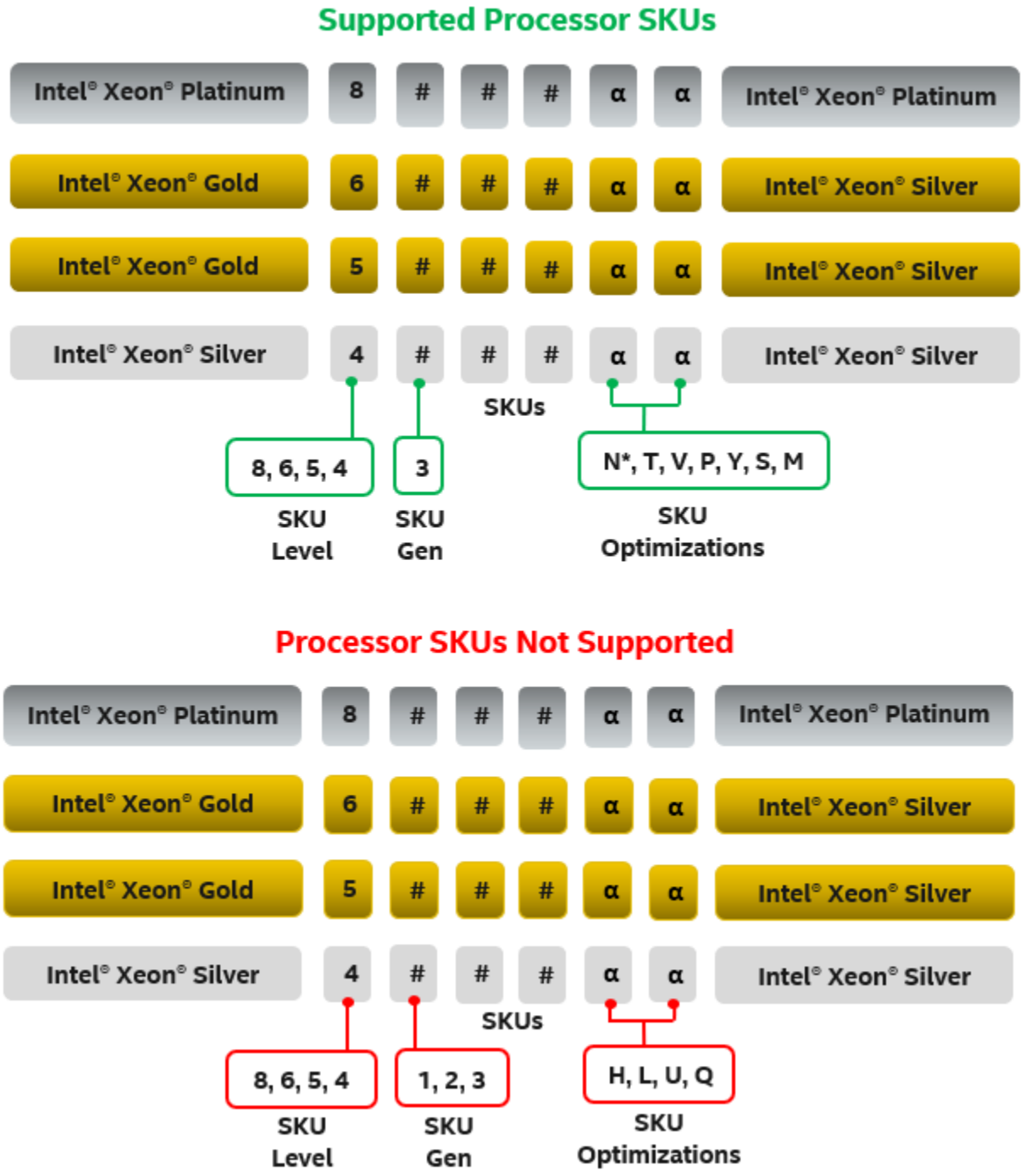


Figure 19. 3rd Gen Intel® Xeon® Scalable Processor Identification

Note: Supported 3rd Gen Intel® Xeon® Scalable processor SKUs must Not end in (H), (L), (U), or (Q). All other processor SKUs are supported.

*** Note:** The 8351N SKU is a 1-socket optimized SKU and is not supported on the Intel® Server Board M50CYP2SB family.

Table 3. 3rd Gen Intel® Xeon® Scalable Processor Family Feature Comparison

Feature	Platinum 8300 Processors	Gold 6300 Processors	Gold 5300 Processors	Silver 4300 Processors
# of Intel® UPI Links	3	3	3	2
Intel® UPI Speed	11.2 GT/s	11.2 GT/s	11.2 GT/s	10.4 GT/s
Supported Topologies	2S-2UPI 2S-3UPI	2S-2UPI 2S-3UPI	2S-2UPI 2S-3UPI	2S-2UPI
Node Controller Support	No	No	No	No
RAS Capability	Advanced	Advanced	Advanced	Standard
Intel® Turbo Boost Technology	Yes	Yes	Yes	Yes
Intel® HT Technology	Yes	Yes	Yes	Yes
Intel® AVX-512 ISA Support	Yes	Yes	Yes	Yes
Intel® AVX-512 - # of 512b FMA Units	2	2	2	2
# of PCIe* Lanes	64	64	64	64
Intel® VMD	Yes	Yes	Yes	Yes

Note: Features may vary between processor SKUs.

See 3rd Gen Intel® Xeon® Scalable processor specifications and product briefs for additional information.

3.3.1 Supported Technologies

The 3rd Gen Intel® Xeon® Scalable processors combine several key system components into a single processor package including the processor cores, Integrated Memory Controller (IMC), and Integrated IO Module.

The core features and technologies for the processor family include:

- Intel® Ultra Path Interconnect (Intel® UPI) – supports up to 11.2 GT/s
- Intel® Speed Shift Technology
- Intel® 64 Architecture
- Enhanced Intel® SpeedStep® Technology
- Intel® Turbo Boost Technology 2.0
- Intel® Hyper-Threading Technology (Intel® HT Technology)
- Intel® Virtualization Technology (Intel® VT-x)
- Intel® Virtualization Technology for Directed I/O (Intel® VT-d)
- Execute Disable Bit
- Intel® Trusted Execution Technology (Intel® TXT)
- Intel® Advanced Vector Extensions (Intel® AVX-512)
- Intel® Advanced Encryption Standard New Instructions (Intel® AES-NI)
- Intel® Deep Learning through VNNI
- Intel® Speed Select Technology on select processor SKUs
- Intel® Resource Director Technology

3.4 Processor Population Rules

Note: The server board may support dual-processor configurations consisting of different processors that meet the following defined criteria. However, Intel does not perform validation testing of this configuration. In addition, Intel does not ensure that a server system configured with unmatched processors will operate reliably. The system BIOS attempts to operate with processors that are not matched but are generally compatible. For optimal system performance in dual-processor configurations, Intel recommends that identical processors be installed.

When using a single processor configuration, the processor must be installed into the processor socket labeled “CPU_0”.

Note: Some server board features may not be functional unless a second processor is installed. For the Intel® Server Board M50CYP2SBSTD, see Figure 16. For the Intel® Server Board M50CYP2SB1U, see Figure 17.

When two processors are installed, the following population rules apply:

- Both processors must have identical extended family, extended model number and processor type
- Both processors must have the same number of cores
- Both processors must have the same cache sizes for all levels of processor cache memory
- Both processors must support identical DDR4 memory frequencies

Note: Processors with different steppings can be mixed in a system as long as the rules mentioned above are met.

Population rules are applicable to any combination of processors within the 3rd Gen Intel® Xeon® Scalable processor family.

For additional information on processor population rules, refer to the *BIOS Firmware External Product Specification (EPS) for the Intel® Server Board D50TNP and M50CYP Families.*

4. Memory Support

This chapter describes the architecture that drives the memory subsystem, supported memory types, memory population rules, and supported memory RAS features.

4.1 Memory Subsystem Architecture

The server board supports up to 32 DDR4 DIMMs, 16 per processor.

The 3rd Gen Intel® Xeon® Scalable processors support eight memory channels using four integrated memory controllers (IMCs). Each memory channel is assigned an identifying letter A-H, with each memory channel supporting two DIMM slots—slot 1 (blue slot) and slot 2 (black slot).

Figure 20. Memory Slot Connectivity

4.2 Supported Memory

The server board supports standard DDR4, RDIMMs, and LDRIMMs and Intel® Optane™ persistent memory 200 series modules.

Server boards designed to support the 3rd Generation Intel® Xeon® Scalable processors may be populated with a combination of both DDR4 DRAM DIMMs and Intel® Optane™ persistent memory 200 series modules.

Note: Previous generation Intel® Optane™ persistent memory modules are not supported.

Intel® Optane™ persistent memory is an innovative technology that delivers a unique combination of affordable large memory capacity and data persistence (non-volatility). It represents a new class of memory and storage technology architected specifically for data center usage. The Intel® Optane™ persistent memory 200 series modules enable higher density (capacity per DIMM) DDR4-compatible memory modules with near-DRAM performance and advanced features not found in standard SDRAM. The persistent memory technology can help boost the performance of data-intensive applications, such as in-memory analytics, databases, content delivery networks, and high performance computing (HPC), as well as deliver consistent service levels at scale with higher virtual machine and container density.

4.2.1 Standard DDR4 DIMM Support

The following figure shows a standard DDR4 DIMM module.

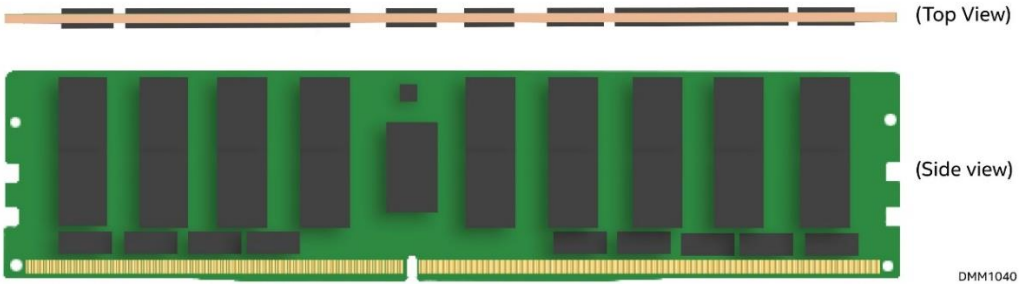


Figure 21. Standard SDRAM DDR4 DIMM Module

The server board supports DDR4 DIMMs with the following features:

- All DDR4 DIMMs must support ECC
- Registered DDR4 (RDIMM), 3DS-RDIMM, Load Reduced DDR4 (LRDIMM), 3DS-LRDIMM
  Note: 3DS = 3 Dimensional Stacking
- RDIMMs and LRDIMMs with thermal sensor On DIMM (TSOD)
- DIMM speeds of up to 3200 MT/s (for 2 DPC)
- DIMM capacities of 8 GB, 16 GB, 32 GB, 64 GB, 128 GB, and 256 GB
- RDIMMs organized as Single Rank (SR), Dual Rank (DR
- 3DS-RDIMM organized as Quad Rank (QR), or Oct Rank (OR)
- LRDIMMs organized as Quad Rank (QR)
- 3DS-LRDIMM organized as Quad Rank (QR), or Oct Rank (OR)

The following tables list the DDR4 DIMM support guidelines.

Table 4. Supported DDR4 DIMM Memory

Type	Ranks per DIMM and Data Width	DIMM Capacity (GB)		Maximum Speed (MT/s) at 1.2 V	
		8 Gb DDR4 Density	16 Gb DDR4 Density	1 DPC	2 DPC
RDIMM	SR x8	8	16	3200	3200[1]
	SR x4	16	32	3200	3200[1]
	DR x8	16	32	3200	3200[1]
	DR x4	32	64	3200	3200[1]
3DS-RDIMM	QR/OR x4	64 (2H) 128 (4H)	128 (2H) 256 (4H)	3200	3200[1]
LRDIMM	QR x4	64	128	3200	3200
3DS-LRDIMM	QR/OR x4	128 (4H)	128 (2H) 256 (4H)	3200	3200

Note: [1] Specification applies only to memory chips mounted by surface mounted technology (SMT) method. For plated through hole (PTH) mounted method, the maximum speed is 2933 MT/s. Refer to the DIMM datasheets for more information.
Note: SR = Single Rank, DR = Dual Rank, QR = Quad Rank, OR = Oct Rank

Table 5. Maximum Supported Standard SDRAM DIMM Speeds by Processor Shelf

Processor Family	Maximum DIMM Speed (MT/s) by Processor Shelf			
	Platinum 8300 Processors	Gold 6300 Processors	Gold 5300 Processors	Silver 4300 Processors
3rd Gen Intel® Xeon® Scalable processor family	3200	3200	2933	2666

Note: Specification applies only to memory chips mounted by surface mounted technology (SMT) method. Refer to the DIMM datasheets for more information.

4.2.2 Intel® Optane™ Persistent Memory 200 Series Module Support

The processor family supports Intel® Optane™ persistent memory 200 series modules. The following figure shows an Intel® Optane™ persistent memory 200 series module.

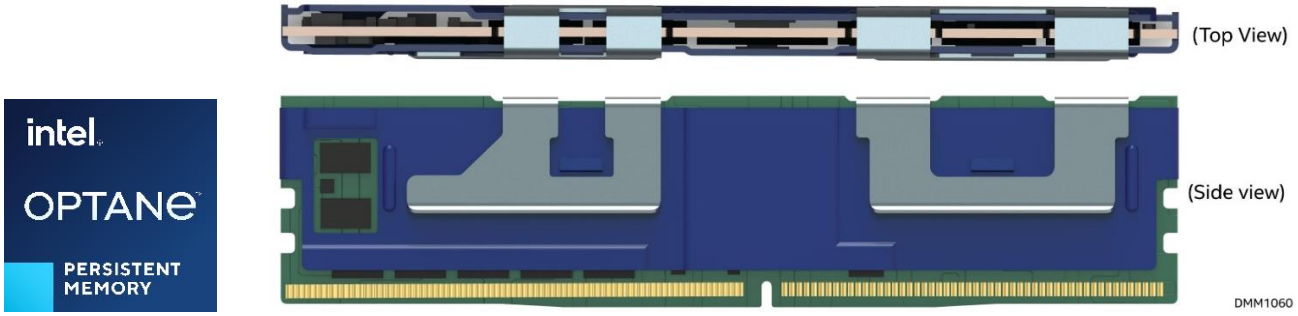


Figure 22. Intel® Optane™ Persistent Memory 200 Series Module

Intel® Optane™ PMem (persistent memory) is an innovative technology that delivers a unique combination of affordable large memory capacity and data persistence (non-volatility). It represents a new class of memory and storage technology architected specifically for data center usage. Intel® Optane™ PMem 200 series enables higher density (capacity per DIMM) DDR4-compatible memory modules with near-DRAM performance and advanced features not found in standard SDRAM.

The module supports the following features:

- Always-enabled AES-256 encryption
- Cache coherent: like DRAM, contains evicted information from the LLC
- Byte-addressable memory
- Higher endurance than enterprise class SSDs

See Section 4.4 for memory RAS features and Intel® Optane™ persistent memory 200 series compatibility with security features Intel® Software Guard Extensions (Intel® SGX), Intel® Total Memory Encryption (Intel® TME), and Intel® Total Memory Encryption – Multi-Tenant (Intel® TME-MT).

Supported operating modes:

- Memory mode (MM)
- App Direct (AD) mode

App Direct mode requires both driver and explicit software support. To ensure operating system compatibility, visit https://www.intel.com/content/www/us/en/architecture-and-technology/optane-memory.html.

4.2.2.1 Intel® Optane™ Persistent Memory 200 Series Module – Memory Mode (MM)

In Memory mode, the standard DDR4 DRAM DIMM acts as a cache for the most frequently accessed data, while Intel® Optane™ persistent memory 200 series modules provide large memory capacity by acting as direct load/store memory. In this mode, applications and operating system are explicitly aware that the Intel® Optane™ persistent memory 200 series is the only type of direct load/store memory in the system. Cache management operations are handled by the integrated memory controller on the Intel® Xeon® Scalable processors. When data is requested from memory, the memory controller first checks the DRAM cache. If the data is present, the response latency is identical to DRAM. If the data is not in the DRAM cache, it is read from the Intel® Optane™ persistent memory 200 series modules with slightly longer latency. The applications with consistent data retrieval patterns that the memory controller can predict, will have a higher cache hit rate. Data is volatile in Memory mode. It will not be saved in the event of power loss. Persistence is enabled in App Direct mode.

4.2.2.2 Intel® Optane™ Persistent Memory 200 Series Module – App Direct (AD) Mode

In App Direct mode, applications and the operating system are explicitly aware that there are two types of direct load/store memory in the platform. They can direct which type of data read or write is suitable for DRAM or Intel® Optane™ persistent memory 200 series modules. Operations that require the lowest latency and do not need permanent data storage can be executed on DRAM DIMM, such as database “scratch pads”. Data that needs to be made persistent or structures that are very large can be routed to the Intel® Optane™ persistent memory. The App Direct mode must be used to make data persistent in memory. This mode requires an operating system or virtualization environment enabled with a persistent memory-aware file system.

App Direct mode requires both driver and explicit software support. To ensure operating system compatibility, visit https://www.intel.com/content/www/us/en/architecture-and-technology/optane-memory.html.

4.2.2.3 Intel® Optane™ PMem configuration using the <F2> BIOS Setup Utility

Following the installation of Intel® Optane™ PMem devices into the system, the devices need to be configured using the <F2> BIOS Setup utility. The BIOS Setup utility includes several Intel® Optane™ PMem configuration options across multiple BIOS Setup screens. The following illustration provides a BIOS Setup screen navigation directing the user to the main Intel® Optane™ PMem configuration screen.

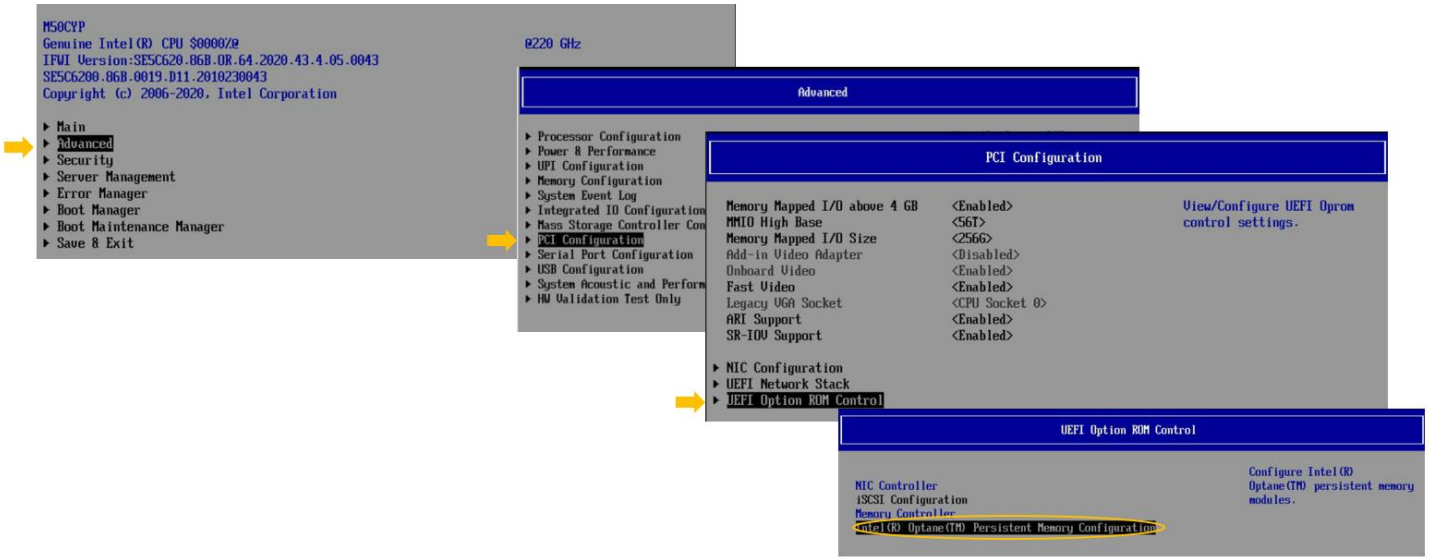


Figure 23. <F2> BIOS Setup Screen Navigation for Intel® Optane™ PMem Setup Options

The main Intel® Optane™ PMem Configuration screen provides links to the various device information and setup screens.

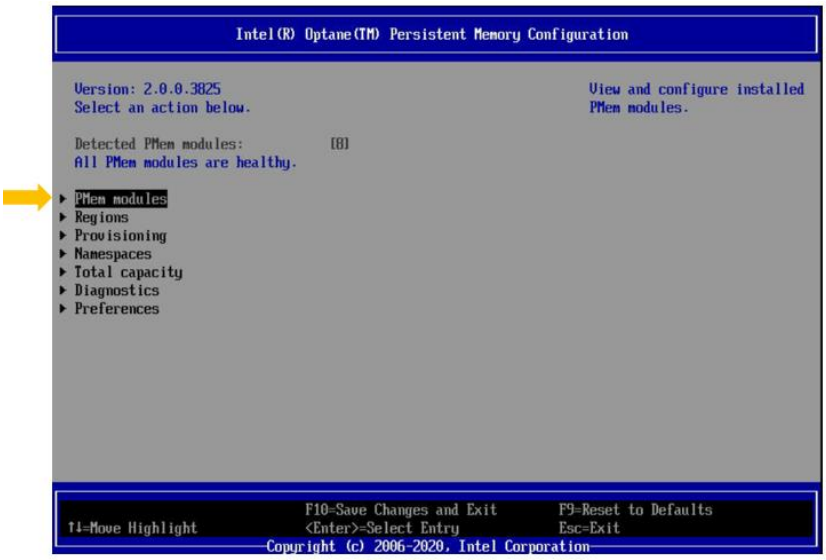


Figure 24. Intel® Optane™ PMem Configuration Menu in <F2> BIOS Setup

4.3 Memory Population

On the server board, a total of 32 memory slots are provided – two slots per channel and eight channels per processor.

This section provides memory population rules and recommendations for standard DD4 DIMMs and Intel® Optane™ persistent memory 200 series modules. The following figure shows the full board layout for all memory slots on both processor sockets.

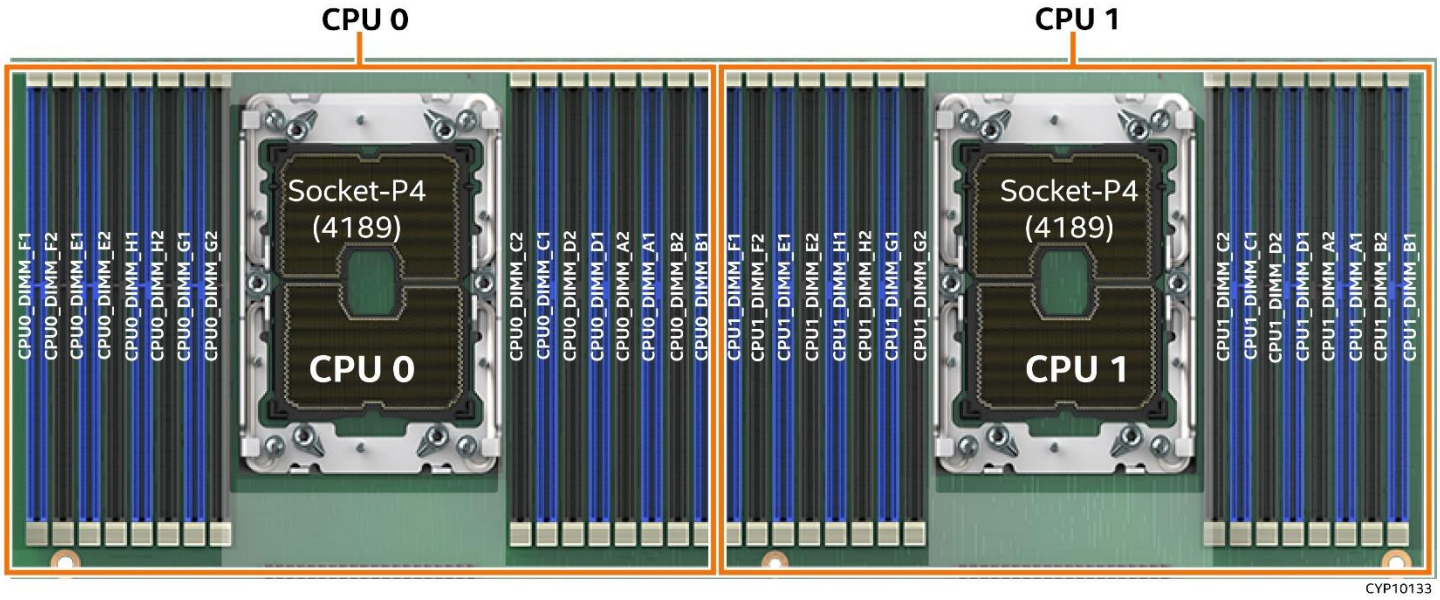


Figure 25. Server Board Memory Slot Layout

4.3.1 DDR4 DIMM Population Rules

Intel DDR4 DIMM Support Disclaimer:

Intel validates and will only provide support for system configurations where all installed DDR4 DIMMs have matching "Identical" or "Like" attributes. See Table 6. A system configured concurrently with DDR4 DIMMs from different vendors will be supported by Intel if all other DDR4 "Like" DIMM attributes match.

Intel does not perform system validation testing nor will it provide support for system configurations where all populated DDR4 DIMMs do not have matching "Like" DIMM attributes as listed in Table 6.

Intel will only provide support for Intel server systems configured with DDR4 DIMMs that have been validated by Intel and are listed on Intel's Tested Memory list for the given Intel server product family.

Intel configures and ships pre-integrated L9 server systems. All DDR4 DIMMs within a given L9 server system as shipped by Intel will be identical. All installed DIMMs will have matching attributes as those listed in the *"Identical" DDR4 DIMM4 Attributes* column in Table 6.

When purchasing more than one integrated L9 server system with the same configuration from Intel, Intel reserves the right to use "Like" DIMMs between server systems. At a minimum, "Like" DIMMS will have matching DIMM attributes as listed in the table below. However, the DIMM model #, revision #, or vendor may be different.

For warranty replacement, Intel will make every effort to ship back an exact match to the one returned. However, Intel may ship back a validated "Like" DIMM. A "Like" DIMM may be from the same vendor but may not be the same revision # or model #, or it may be an Intel validated DIMM from a different vendor. At a minimum, all "Like" DIMMs shipped from Intel will match attributes of the original part according to the definition of "Like" DIMMs in the following table.

Table 6. DDR4 DIMM Attributes Table for "Identical" and "Like" DIMMs

- DDR4 DIMMs are considered "Identical" when ALL listed attributes between the DIMMs match
- Two or more DDR4 DIMMs are considered "Like" DIMMs when all attributes minus the Vendor, and/or DIMM Part # and/or DIMM Revision#, are the same.

Attribute	"Identical" DDR4 DIMM Attributes	"Like" DDR4 DIMM Attributes	Possible DDR4 Attribute Values
Vendor	**Match**	**Maybe Different**	Memory Vendor Name
DIMM Part #	**Match**	**Maybe Different**	Memory Vendor Part #
DIMM Revision #	**Match**	**Maybe Different**	Memory Vendor Part Revision #
SDRAM Type	**Match**	**Match**	DDR4
DIMM Type	**Match**	**Match**	RDIMM, LRDIMM
Speed (MHz)	**Match**	**Match**	2666, 2933, 3200
Voltage	**Match**	**Match**	1.2V
DIMM Size (GB)	**Match**	**Match**	8GB, 16GB, 32GB, 64GB, 128GB, 256GB
Organization	**Match**	**Match**	1Gx72; 2Gx72; 4Gx72; 8Gx72; 16Gx72; 32Gx72
DIMM Rank	**Match**	**Match**	1R, 2R, 4R, 8R
DRAM Width	**Match**	**Match**	x4, x8
DRAM Density	**Match**	**Match**	8Gb, 16Gb

Note: Although mixed DDR4 DRAM DIMM configurations are supported, Intel only performs platform validation on systems that are configured with identical DRAM DIMMs installed.

The following memory population rules apply when installing DDR4 DIMMs:

- Mixing rules:
  - Mixing DDR4 DIMMs of different frequencies and latencies is not supported within or across processors. If a mixed configuration is encountered, the BIOS attempts to operate at the highest common frequency and the lowest latency possible.
  - x4 and x8 DIMMs may be mixed in the same channel.
  - Mixing of DDR4 DIMM types (RDIMM, LRDIMM, 3DS-RDIMM, 3DS-LRDIMM) within or across processors is not supported. This is a Fatal Error Halt in Memory Initialization.
- For a single DDR4 DIMM in a dual-slot channel, populate slot 1 (blue slot).
- For multiple DDR4 DIMMs per channel:
  - When populating a quad-rank DDR4 DIMM with a single- or dual-rank DDR4 DIMM in the same channel, the quad-rank DDR4 DIMM must be populated farthest from the processor. Incorrect DIMM placement results in an MRC error code. A maximum of 8 logical ranks can be used on any one channel, as well as a maximum of 10 physical ranks loaded on a channel.
  - For RDIMM, LRDIMM, 3DS-RDIMM, and 3DS-LRDIMM, always populate DIMMs with higher electrical loading in slot 1 (blue slot) followed by slot 2 (black slot).
- Memory slots associated with a given processor are unavailable if the corresponding processor socket is not populated.
- Processor sockets are self-contained and autonomous. However, all memory subsystem support (such as memory RAS and error management) in the BIOS Setup are applied commonly for each installed processor.
- For best system performance, memory must be installed in all eight channels for each installed processor.
- For best system performance in dual processor configurations, installed DDR4 DIMM type and population for DDR4 DIMMs configured to CPU 1 must match DDR4 DIMM type and population configured to CPU 0. For additional information, see Section 4.3.3.

4.3.2 Intel® Optane™ Persistent Memory 200 Series Module Rules

All operating modes:

- Only Intel® Optane™ persistent memory 200 series modules are supported.
- Intel® Optane™ persistent memory 200 series modules of different capacities cannot be mixed within or across processor sockets.
- Memory slots supported by integrated memory controller 0 (memory channels A and B) of a given processor must be populated before memory slots on other IMCs.
- For multiple DIMMs per channel:
  - Only one Intel® Optane™ persistent memory 200 series module is supported per memory channel.
  - Intel® Optane™ persistent memory 200 series modules are supported in either DIMM slot when mixed with LRDIMM or 3DS-LRDIMM.
  - Intel® Optane™ persistent memory 200 series modules are only supported in DIMM slot 2 (black slot) when mixed with RDIMM or 3DS-RDIMM.
- No support for SDRAM SRx8 DIMM that is populated within the same channel as the Intel® Optane™ persistent memory 200 series module in any operating mode.
- Ensure the same DDR4 DIMM type and capacity is used for each DDR4 + Intel® Optane™ persistent memory 200 series module combination.

Memory mode:

- Populate each memory channel with at least one DRAM DIMM to maximize bandwidth.
- Intel® Optane™ persistent memory 200 series modules must be populated symmetrically for each installed processor (corresponding slots populated on either side of each processor).

App Direct mode:

- Minimum of one DDR4 DIMM per IMC (IMC 0, IMC 1, IMC 2 and IMC 3) for each installed processor.
- Minimum of one Intel® Optane™ persistent memory 200 series module for the board.
- Intel® Optane™ persistent memory 200 series modules must be populated symmetrically for each installed processor (corresponding slots populated on either side of each processor).

Table 7. Intel® Optane™ Persistent Memory 200 Series Module Support

Processor Shelf	Intel® Optane™ Persistent Memory 200 Series Capacity (GB)	Speed (MT/s)
Silver 4300 processors	128 256 512	2666 2400
Gold 5300 processors	128 256 512	2933 2666 2400
Gold 6300 Processors	128 256 512	3200 2933 2666 2400
Platinum 8300 processors	128 256 512	3200 2933 2666 2400

Table 8. Standard DDR4 DIMMs Compatible with Intel® Optane™ Persistent Memory 200 Series Module

Type	Ranks per DIMM and Data Width	DIMM Size (GB)	
		8 Gb DRAM density	16 Gb DRAM density
RDIMM **(PTH – up to 2933 MT/s)** **(SMT – up to 3200 MT/s)**	SR x8	N/A	N/A
	SR x4	16	32
	DR x8	16	32
	DR x4	32	64
3DS-RDIMM **(PTH – up to 2933 MT/s)** **(SMT – up to 3200 MT/s)**	QR x4	N/A	128 (2H)
	OR x4	N/A	256 (4H)
LRDIMM **(PTH/SMT – up to 3200 MT/s)**	QR x4	64	128
3DS-LRDIMM **(PTH/SMT – up to 3200 MT/s)**	QR x4	N/A	N/A
	OR x4	128 (4H)	256 (4H)

Note: SR = Single Rank, DR = Dual Rank, QR = Quad Rank, OR = Oct Rank, H = Stack Height, PTH = Plated Through Hole, SMT = Surface-Mount Technology

4.3.3 Recommended Memory Configurations

This section provides the recommended memory population configurations for the server board. For best system performance in dual-processor configurations, installed memory type and population should be the same for both processors.

See the following figure to identify the memory slot locations and the following two tables for recommended population configurations.

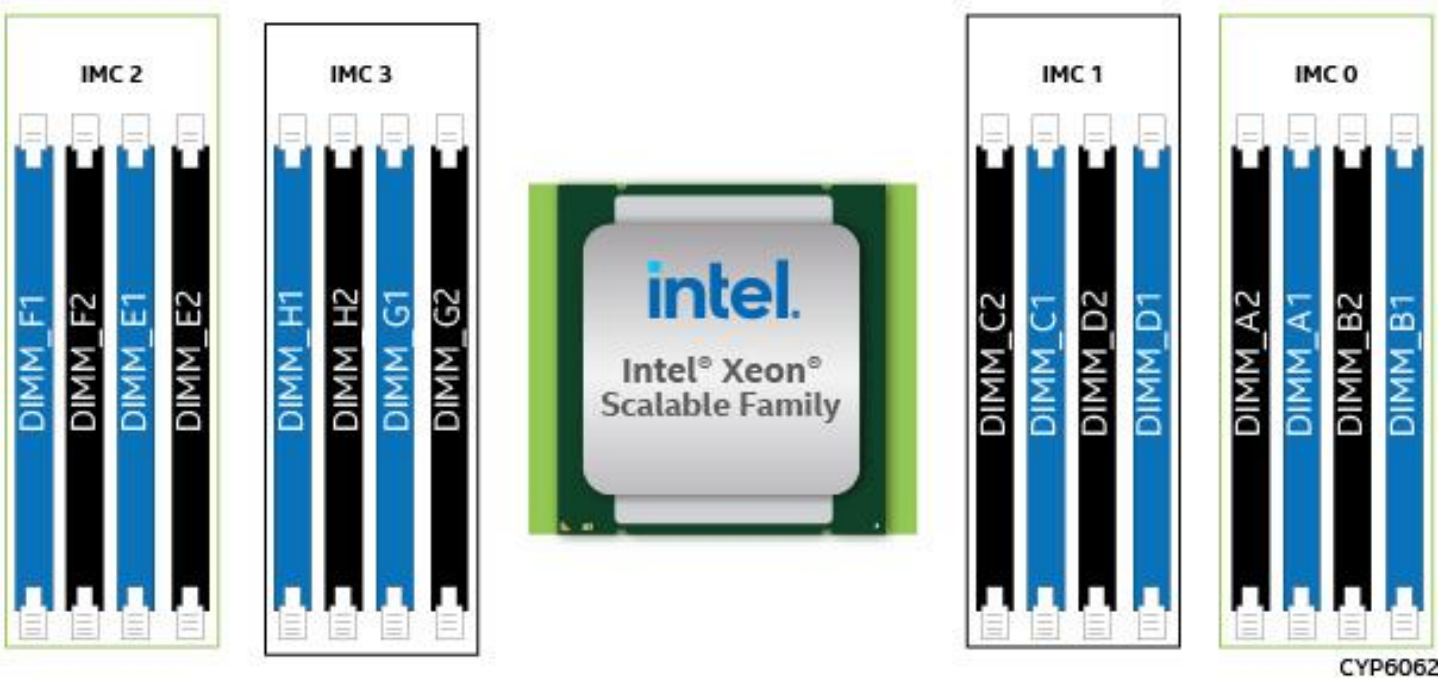


Figure 26. Memory Slot Identification

Table 9. Standard DDR4 DIMM-Only per Socket Population Configurations

# of DIMMs	IMC2				IMC3				IMC1				IMC0			
	CH F		CH E		CH H		CH G		CH C		CH D		CH A		CH B	
	Slot 1	Slot 2	Slot1	Slot2	Slot 1	Slot 2	Slot 1	Slot 2	Slot 2	Slot 1	Slot 2	Slot 1	Slot 2	Slot 1	Slot 2	Slot 1
1	–	–	–	–	–	–	–	–	–	–	–	–	–	DRAM	–	–
2	–	–	DRAM	–	–	–	–	–	–	–	–	–	–	DRAM	–	–
4	–	–	DRAM	–	–	–	DRAM	–	–	DRAM	–	–	–	DRAM	–	–
6	DRAM	–	DRAM	–	–	–	DRAM	–	–	DRAM	–	–	–	DRAM	–	DRAM
8	DRAM	–	DRAM	–	DRAM	–	DRAM	–	–	DRAM	–	DRAM	–	DRAM	–	DRAM
12	DRAM	DRAM	DRAM	DRAM	–	–	DRAM	DRAM	DRAM	DRAM	–	–	DRAM	DRAM	DRAM	DRAM
12	DRAM	–	DRAM	DRAM	DRAM	–	DRAM	DRAM	DRAM	DRAM	–	DRAM	DRAM	DRAM	–	DRAM
16	DRAM	DRAM	DRAM	DRAM	DRAM	DRAM	DRAM	DRAM	DRAM	DRAM	DRAM	DRAM	DRAM	DRAM	DRAM	DRAM

Table 10. Standard DDR4 DIMM and Intel® Optane™ Persistent Memory 200 Series Module (PMem) Population Configurations

DRAM / PMem	Mode	IMC2				IMC3				IMC1				IMC0			
		CH F		CH E		CH H		CH G		CH C		CH D		CH A		CH B	
		Slot 1	Slot 2	Slot 1	Slot 2	Slot 1	Slot 2	Slot 1	Slot 2	Slot 2	Slot 1	Slot 2	Slot 1	Slot 2	Slot 1	Slot 2	Slot 1
8 DRAM/ 8 PMem	AD or MM	DRAM	PMem	DRAM	PMem	DRAM	PMem	DRAM	PMem	PMem	DRAM	PMem	DRAM	PMem	DRAM	PMem	DRAM
8 DRAM/ 4 PMem	AD or MM	DRAM	–	DRAM	PMem	DRAM	–	DRAM	PMem	PMem	DRAM	–	DRAM	PMem	DRAM	–	DRAM
4 DRAM/ 4 PMem	AD or MM	PMem	–	DRAM	–	PMem	–	DRAM	–	–	DRAM	–	PMem	–	DRAM	–	PMem
		DRAM	–	PMem	–	DRAM	–	PMem	–	–	PMem	–	DRAM	–	PMem	–	DRAM
6 DRAM/ 1 PMem	AD	DRAM	–	DRAM	–	–	–	DRAM	–	–	DRAM	–	PMem	–	DRAM	–	DRAM
		–	–	DRAM	–	DRAM	–	DRAM	–	–	DRAM	–	DRAM	–	DRAM	–	PMem
		DRAM	–	DRAM	–	PMem	–	DRAM	–	–	DRAM	–	–	–	DRAM	–	DRAM
		PMem	–	DRAM	–	DRAM	–	DRAM	–	–	DRAM	–	DRAM	–	DRAM	–	–
8 DRAM/ 1 PMem	AD	DRAM	–	DRAM	–	DRAM	–	DRAM	–	–	DRAM	–	DRAM	PMem	DRAM	–	DRAM
		DRAM	–	DRAM	–	DRAM	–	DRAM	–	PMem	DRAM	–	DRAM	–	DRAM	–	DRAM
		DRAM	–	DRAM	PMem	DRAM	–	DRAM	–	-	DRAM	–	DRAM	–	DRAM	–	DRAM
		DRAM	–	DRAM	–	DRAM	–	DRAM	PMem	-	DRAM	–	DRAM	–	DRAM	–	DRAM
12 DRAM/ 2 PMem	AD	DRAM	DRAM	DRAM	DRAM	PMem	–	DRAM	DRAM	DRAM	DRAM	–	PMem	DRAM	DRAM	DRAM	DRAM
		DRAM	DRAM	DRAM	DRAM	PMem	–	DRAM	DRAM	DRAM	DRAM	–	PMem	DRAM	DRAM	DRAM	DRAM

Note: AD = App Direct mode, MM = Memory mode, PMem = Persistent Memory Module

Notes on Intel® Optane™ persistent memory 200 series module population:

- For MM, recommended ratio of standard DRAM capacity to Intel® Optane™ persistent memory 200 series module capacity is between 1 GB:4 GB and 1 GB:16 GB.
- For each individual population, rearrangements between channels are allowed as long as the resulting population is consistent with defined memory population rules.
- For each individual population, the same DDR4 DIMM must be used in all slots, as specified by the defined memory population rules.

4.4 Memory RAS Support

Processors within the3rd Gen Intel® Xeon® Scalable processor family support the standard or advanced memory RAS features, depending on processor SKU, defined in Table 11. This table lists the RAS features pertaining to system memory that has standard DDR4 DIMMs or a combination of standard DDR4 DIMMS and Intel® Optane™ persistent memory 200 series modules. These features are managed by the processor's IMC.

Table 11. Memory RAS Features

Memory RAS Feature	Description	Standard	Advanced
Partial Cache-Line Sparing (PCLS)	Allows replacing failed single bit within a device using spare capacity available within the processor's integrated memory controller (IMC). Up to 16 failures allowed per memory channel and no more than one failure per cache line. After failure is detected, replacement is performed at a nibble level. Supported with x4 DIMMs only.	√	√
Device Data Correction	Single Device Data Correction (SDDC) via static virtual lockstep Supported with x4 DIMMs only.	√	√
	Adaptive Data Correction – Single Region (ADC-SR) via adaptive virtual lockstep (applicable to x4 DRAM DIMMs). Cannot be enabled with "Memory Multi-Rank Sparing" or "Write Data CRC Check and Retry."	√	√
	Adaptive Double Data Correction – Multiple Region (ADDDC-MR, + 1) Supported with x4 DIMMs only.	–	√
DDR4 Command/Address (CMD/ADDR) Parity Check and Retry	DDR4 technology based CMD/ADDR parity check and retry with CMD/ADDR parity error "address" logging and CMD/ADDR retry.	√	√
DDR4 Write Data CRC Check and Retry	Checks for CRC mismatch and sends a signal back to the processor for retry. Cannot be enabled with "ADC-SR" or "ADDDC-MR, +1."	√	√
Memory Data Scrambling with Command and Address	Scrambles the data with address and command in "write cycle" and unscrambles the data in "read cycle". Addresses reliability by improving signal integrity at the physical layer. Additionally, assists with detection of an address bit error.	√	√
Memory Demand and Patrol Scrubbing	Demand scrubbing is the ability to write corrected data back to the memory once a correctable error is detected on a read transaction. Patrol scrubbing proactively searches the system memory, repairing correctable errors. Prevents accumulation of single-bit errors.	√	√
Memory Mirroring	Full memory mirroring: An intra-IMC method of keeping a duplicate (secondary or mirrored) copy of the contents of memory as a redundant backup for use if the primary memory fails. The mirrored copy of the memory is stored in memory of the same processor socket's IMC. Dynamic (without reboot) failover to the mirrored DIMMs is transparent to the operating system and applications.	√	√
	Address range/partial memory mirroring: Provides further intra socket granularity to mirroring of memory. This allows the firmware or OS to determine a range of memory addresses to be mirrored, leaving the rest of the memory in the socket in non-mirror mode.	–	√
DDR Memory Multi-Rank Memory Sparing	Up to two ranks out of a maximum of eight ranks can be assigned as spare ranks. Cannot be enabled with "ADC-SR", "ADDDC-MR, +1", and "Memory Mirroring".	√	√
Memory SMBus* Hang Recovery	Allows system recovery if the SMBus fails to respond during runtime, thus, preventing system crash.	√	√
Memory Disable and Map Out for Fault Resilient Boot (FRB)	Allows memory initialization and booting to the operating system even when memory fault occurs.	√	√
Post Package Repair (PPR)	PPR offers additional spare capacity within the DDR4 DRAM that can be used to replace faulty cell areas detected during system boot time.	√	√
Memory Thermal Throttling	Management controller monitors the memory DIMM temperature and can temporarily slow down the memory access rates to reduce the DIMM temperature if needed.	√	√

Memory RAS Feature	Description	Standard	Advanced
MEMHOT Pin Support for Error Reporting	MEMHOT pin can be configured as an output and used to notify if DIMM is operating within the target temperature range. Used to implement "Memory Thermal Throttling".	√	√

Notes: Population Rules and BIOS Setup for Memory RAS

- Memory sparing and memory mirroring options are enabled in BIOS Setup.
- Memory sparing and memory mirroring options are mutually exclusive in this product. Only one operating mode at a time may be selected in BIOS Setup.
- If a RAS mode has been enabled and the memory configuration is not able to support it during boot, the system will fall back to independent channel mode and log and display errors.
- Rank sparing mode is only possible when all channels that are populated with memory have at least two single-rank or double-rank DIMMs installed, or at least one quad-rank DIMM installed on each populated channel.
- Memory mirroring mode requires that for any channel pair that is populated with memory, the memory population on both channels of the pair must be identically sized.
- The Intel® Optane™ persistent memory 200 series RAS features listed in the following table are integrated into the system memory RAS features.

The following table lists additional memory RAS features specific to the Intel® Optane™ persistent memory 200 series memory. These features are managed by the processor's IMC.

Table 12. Intel® Optane™ Persistent Memory 200 Series RAS Features

Memory RAS Feature	Description
DIMM Error Detection and Correction	Protects against random bit failures across media devices.
DIMM Device Failure Recovery (Single Device Data Correction (SDDC))	Corrects errors resulting from the failure of a single media device.
DIMM Package Sparing (Double Device Data Correction (DDDC))	Achieved by a spare device on the DIMM and erasure decoding.
DIMM Patrol Scrubbing	Proactively searches the DIMM memory, repairing correctable errors. This can prevent correctable errors from becoming uncorrectable due to accumulation of failed bits.
DIMM Address Error Detection	Ensures the correctness of addresses when data is read from media devices.
DIMM Data Poisoning	Mechanism to contain, and possibly recover from, uncorrectable data errors. Depending on the mode used, poisoning has different reset behavior: • In Memory mode, poison is cleared after reset. • In App Direct mode, poison is not cleared with reset.
DIMM Viral	Ensures that potentially corrupted data is not committed to persistent memory in App Direct and is supported only in tandem with poison. Viral mode does not apply to memory mode.
DIMM Address Range Scrub (ARS)	Obtains the healthy memory media range before assigning it to a persistent memory region.
DDR-T Command and Address Parity Check and Retry	Host retries a CMD/ADDR transaction if the DIMM controller detects a parity error and initiates an error flow.
DDR-T Read Write Data ECC Check and Retry	Host continuously retries a data transaction as long as the DIMM controller detects an ECC error and initiates an error flow.
Faulty DIMM Isolation	Identifies a specific failing DIMM enabling replacement of only the DIMM that has failed.

The Intel® Server Board M50CYP2SB family security feature support includes Intel® Software Guard Extensions (Intel® SGX), Intel® Total Memory Encryption (Intel® TME), and Intel® Total Memory Encryption – Multi-Tenant (Intel® TME-MT). When any of these security features are enabled, Intel® Optane™ PMem 200 Series will be disabled. In addition, some of the memory RAS features will be disabled as indicated in the following table.

Table 13. Compatibility of RAS features Intel® SGX, Intel® TME, and Intel® TME-MT

Feature/Technology	Intel® SGX	Intel® TME, Intel® TME-MT
Intel® Optane™ persistent memory 200 series	No	No
ADC(SR)/ADDDC(MR)	No	Yes
MCA Recovery – Execution Path	No	Yes
MCA Recovery – Non-execution Path	Yes	Yes
Address Range Mirroring	No	Yes
Dynamic Capacity change: CPU/Memory/IIO, Physical CPU Board Hot Add/Remove, OS CPU/Memory/IIO On-lining (Capacity change), OS CPU off-lining (Capacity change), Intel® UPI link Hot pluggability, and Intel® UPI System Quiescence.	No	Yes
Static/Hard Partitioning, Electronically Isolated (Static/Hard) Partitioning, Dynamic Partitioning (Via Resource/Capacity Addition), Multiple South Bridge (PCH) Presence for supporting system partitioning	No	Yes

5. Server Management

The Intel® Server Board M50CYP2SB family uses the baseboard management controller (BMC) features of an ASpeed* AST2500 server management processor. The BMC supports multiple system management features including intra-system sensor monitoring, fan speed control, system power management, and system error handling and messaging. It also provides remote platform management capabilities including remote access, monitoring, logging, and alerting features.

In support of system management, the system includes a dedicated management port and support for two system management tiers and optional system management software.

- Standard management features (Included)
- Advanced management features ($$ Optional)
- Intel® Data Center Manager (DCM) support ($$ Optional)

The following subsections provide a brief description of each.

5.1 Remote Management Port

The server board includes a dedicated 1 Gb/s RJ45 management port used to access embedded system management features remotely.

Note: The management port is dedicated for system management access purposes only. The port is not intended or designed to support standard LAN data traffic.

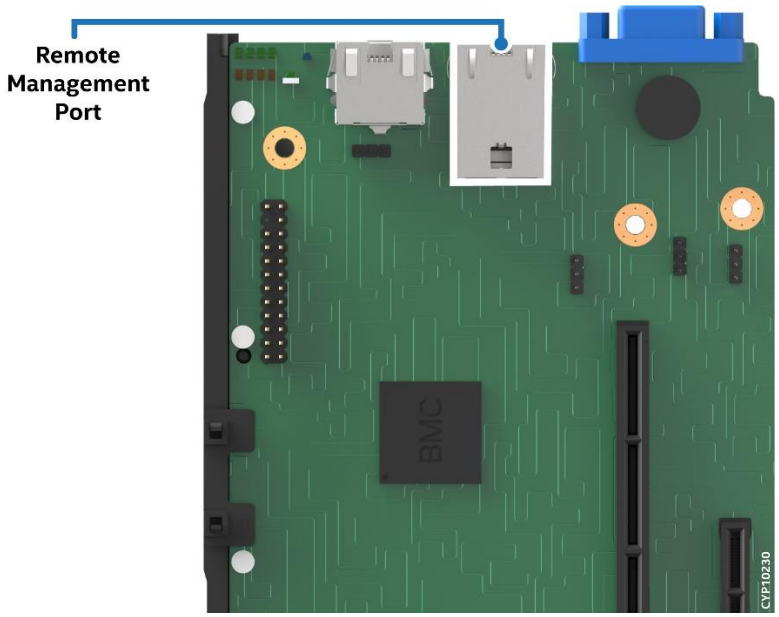


Figure 27. Remote Management Port

To access the server remotely using the management port requires network parameters to be configured using the <F2> BIOS Setup utility.

5.1.1 Configuring System Management Port Using <F2> BIOS Setup

1. During the system power-on POST process, press **<F2>** when prompted to go to the BIOS Setup utility main menu page.
2. Navigate to the ***Server Management*** tab and select ***BMC LAN Configuration*** to enter the BMC LAN Configuration screen (Figure 28).

Figure 28. BIOS Setup BMC LAN Configuration Screen

3. The system is configured using the **BMC Dedicated Network Configuration**
4. For an IPv4 network:
   - If configuring the server management BMC LAN, scroll to **Baseboard LAN configuration** > **IP source** and then select either **Static** or **Dynamic**. If **Static** is selected, configure the **IP address**, **Subnet mask**, and **Gateway IP** as needed.
5. For an IPv6 network:
   - If configuring the server management BMC LAN, scroll to **Baseboard LAN IPv6 configuration** > **IP source** and then select **Enabled**. Then scroll to **IPV6 source** and select either **Static** or **Dynamic**. If **Static** is selected, configure the **IPV6 address**, **Gateway IPV6**, and **IPV6 Prefix Length** as needed.
6. The default **User Name** and **Password** is **admin/admin**.
7. If there is a need to change the User and Password, select **BMC User Settings** to enter the User Configuration screen (Figure 29).
8. Under **Add User**, set the following settings as desired:
   - **User Name** – Enter the desired name. Note that the anonymous user cannot be changed.
   - **User password** – Enter the desired password twice.
   - **Channel No** – Select the Channel
   - **Privilege** – Select the privilege to be used. (Administrator privilege is required to use KVM or media redirection)
9. Press **<F10>** to save the configured settings and exit BIOS Setup. The server reboots with the new LAN settings.

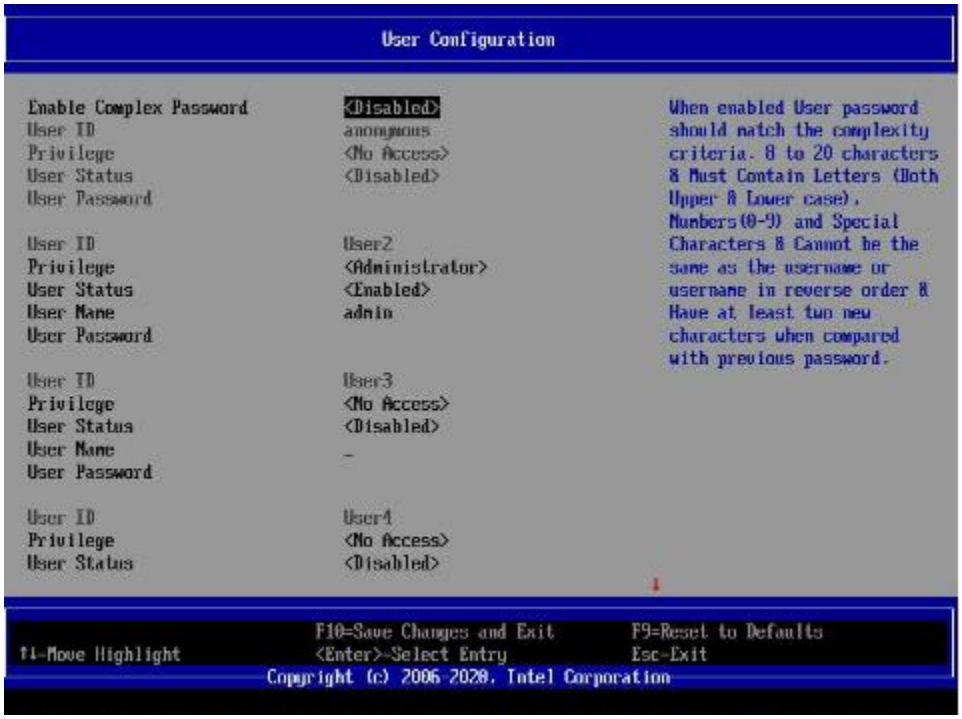


Figure 29. BIOS Setup User Configuration Screen

Once the management port is configured, the server can be accessed remotely to perform system management features defined in the following sections.

5.2 Standard System Management Features

The following system management features are supported on the Intel® Server Board M50CYP2SB family by default.

- Virtual KVM over HTML5
- Integrated BMC Web Console
- Redfish
- IPMI 2.0
  - Node Manager
- Out-of-band BIOS/BMC Update and Configuration
- System Inventory
- Autonomous Debug Log

The following subsections provide a brief description for each feature.

5.2.1 Virtual KVM over HTML5

The BMC firmware supports keyboard, video, and mouse redirection (KVM) over LAN. This feature is available remotely from the embedded web server as an HTML5 application. USB1.1 or USB 2.0 based mouse and keyboard redirection are supported. The KVM-redirection (KVM-r) session can be used concurrently with media-redirection (media-r). This feature allows a user to interactively use the keyboard, video, and mouse (KVM) functions of the remote server as if the user were physically at the managed server.

KVM redirection consoles support the following keyboard layouts: English, Chinese (traditional), Japanese, German, French, Spanish, Korean, Italian, and United Kingdom. KVM redirection includes a “soft keyboard” function. The “soft keyboard” is used to simulate an entire keyboard that is connected to the remote system.

The “soft keyboard” functionality supports the following layouts: English, Dutch, French, German, Italian, Russian, and Spanish.

The KVM-redirection feature automatically senses video resolution for best possible screen capture and provides high-performance mouse tracking and synchronization. It allows remote viewing and configuration in pre-boot POST and BIOS Setup once BIOS has initialized video.

5.2.2 Integrated Baseboard Management Controller Web Console (Integrated BMC Web Console)

The BMC firmware has an embedded web server that can remotely serve web pages to any supported browser. This web console allows administrator to view system information including firmware versions, server health, diagnostic information, power statistics. The web console enables configuration of the BMC and BIOS. It provides the ability for users to perform power actions, launch KVM and set up virtual media redirection.

Enter the configured IP address of the BMC management port into the web browser to open the Integrated BMC Web Console module login page (See Figure 30). To use a secure connection, type:

```
https://<IPaddress_or_Hostname>/
```

Enter the username and password and select a language option. For example:

- Username: `root`
- Password: `superuser`
- Language: **English**

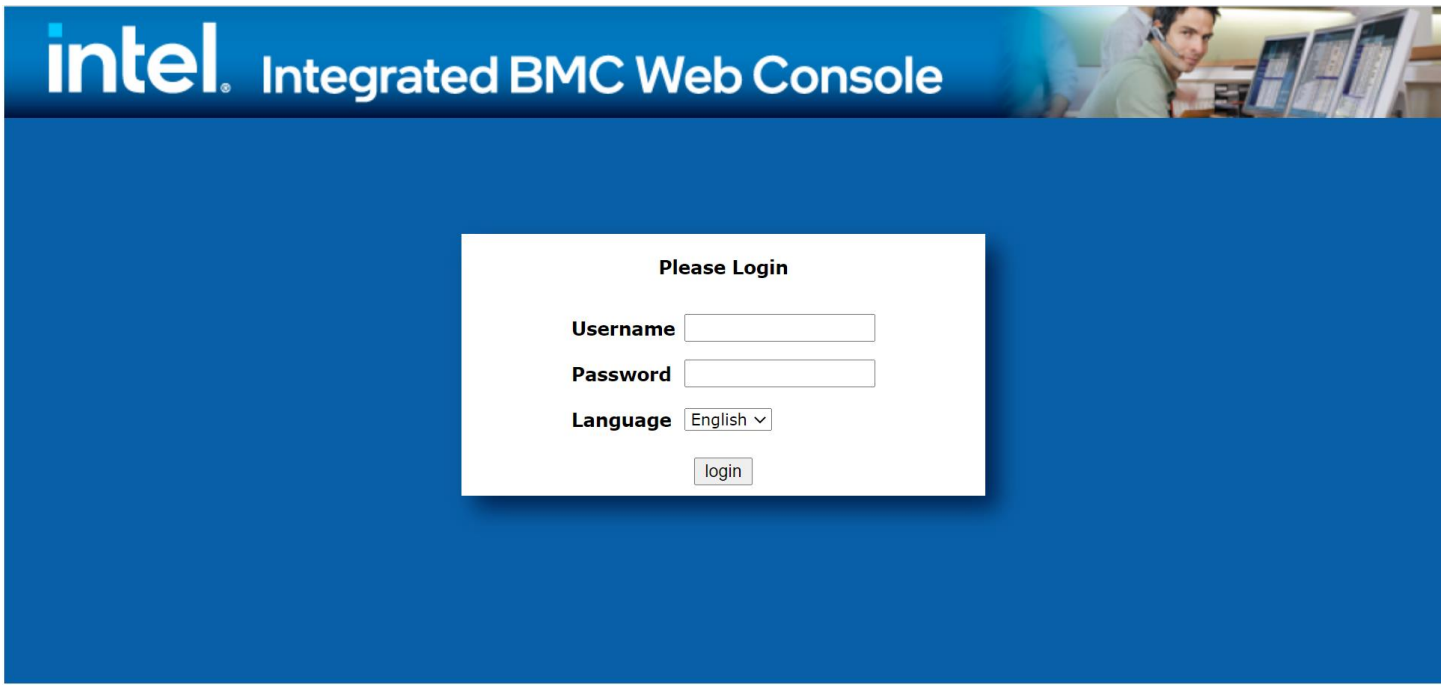


Figure 30. Integrated BMC Web Console Login Page

Click the **Login** button to view the homepage.

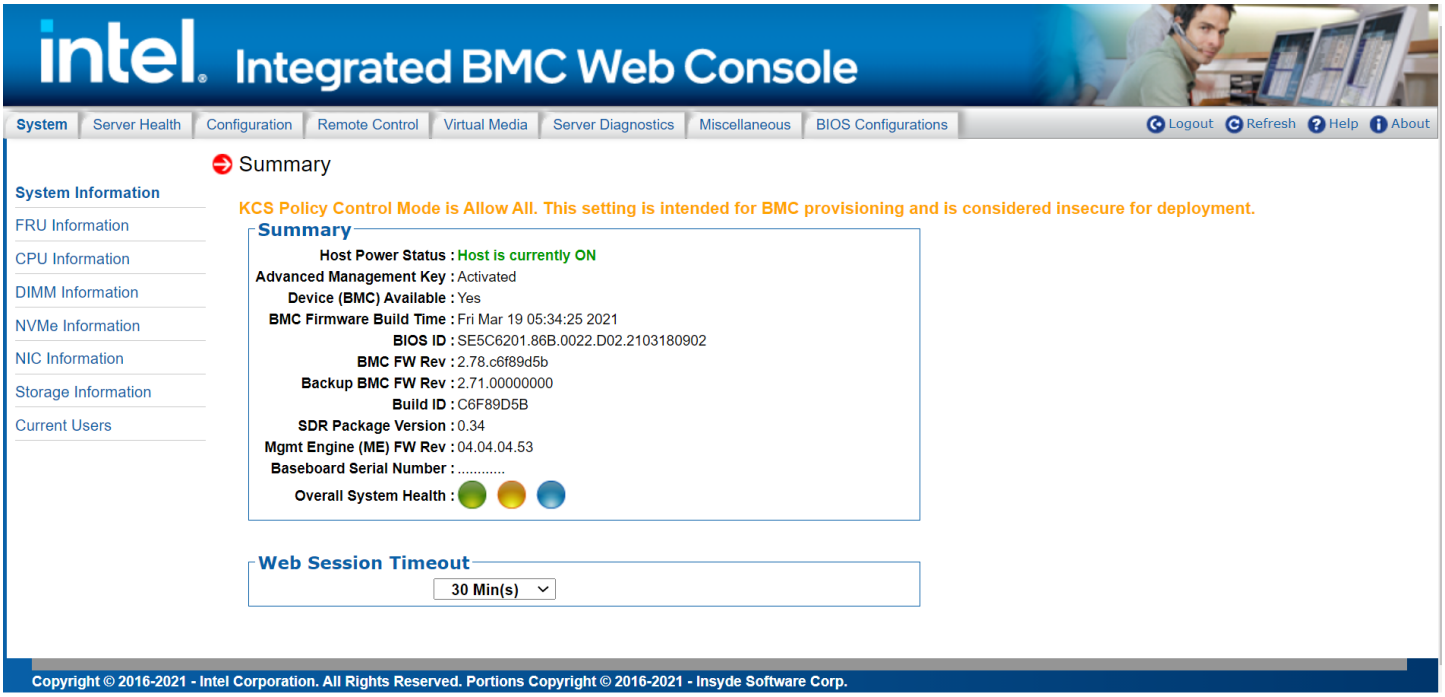


Figure 31. Integrated BMC Web Console – Main Console View

For setup and additional information about this utility, download the *Intel® Integrated Baseboard Management Controller Web Console (Integrated BMC Web Console) User Guide for the Intel® Server Board D50TNP and M50CYP Families*.

5.2.3 Redfish* Support

The BMC currently supports version 1.7 and schema version 2019.1. DMTF's Redfish* is a standard designed to deliver simple and secure management for converged, hybrid IT and the Software Defined Data Center (SDDC). Both human readable and machine capable, Redfish leverages common Internet and web services standards to expose information directly to the modern tool chain.

5.2.4 IPMI 2.0 Support

The BMC is IPMI 2.0 compliant including support for Intel® Dynamic Power Node Manager. IPMI defines a set of interfaces used by system administrators for out-of-band management of computer systems and monitoring of their operation.

5.2.5 Out-of-Band BIOS / BMC Update and Configuration

The BMC supports Redfish schemas and embedded web console features that allow administrators to update the BMC, BIOS, Intel ME and SDR firmware. The BMC firmware also includes Power Supply and Back plan firmware. The BMC update will happen immediately and cause a BMC reset to occur at the end. The BIOS and Intel ME firmware is staged in the BMC and will be updated on the next reboot. The BMC also supports Redfish and embedded web console feature to view and modify BIOS settings. On each boot, BIOS provides all its settings and active value to the BMC to be displayed. BIOS also checks if any changes are requested and performs those changes.

5.2.6 System Inventory

The BMC supports Redfish schemas and embedded web console pages to display system inventory. This inventory includes FRU information, CPU, Memory, NVMe, networking, and storage. When applicable, the firmware version will also be provided.

5.2.7 Autonomous Debug Log

The BMC has a debug log that can be downloaded to facilitate support issues. This debug log can be downloaded from the embedded web console or via syscfg and SDPTool utilities. The debug log contains configuration data including SDR, SEL, BMC configuration, PCI configuration, power supply configuration and power supply black box data. The debug log also contains SMBIOS data and the POST codes from the last two system boots. Finally, when the system has a catastrophic error condition leading to a system shutdown, the BMC will hold the CPU in reset long enough to collect processor machine check registers, memory controller machine check registers, I/O global error registers, and other processor state info.

5.2.8 Security Features

The BMC contains several security features including OpenLDAP and Active Directory, security logs, ability to turn off any remote port, SSL certificate upload, VLAN support, and KCS control. The BMC also supports full user management with the ability to define password complexity rules. Each BMC release is given a security version number to prevent firmware downgrades from going to lower security versions. Intel provides a best practices security guide, available at
https://www.intel.com/content/www/us/en/support/articles/000055785/server-products.html

5.3 Advanced System Management Features

Purchasing an optional Advanced System Management product key (iPC ADVSYSMGMTKEY), unlocks the following advanced system management features:

- Virtual Media Image Redirection (HTML5 and Java)
- Virtual Media over network share and local folder
- Active Directory support
- Included single system license for Intel® Data Center Manager (Intel® DCM)
  - Intel® Data Center Manager (Intel® DCM) is a software solution that collects and analyzes the real-time health, power, and thermals of a variety of devices in data centers helping you improve the efficiency and uptime. For more information, go to https://www.intel.com/content/www/us/en/software/intel-dcm-product-detail.html
- Future Feature Additions – Tentative availability Q4 2021
  - ❖ Full system firmware update including drives, memory, and RAID
  - ❖ Storage and network device monitoring
  - ❖ Out-of-band hardware RAID Management for latest Intel RAID cards

The Advanced System Management product key can be purchased and pre-loaded onto the system when ordering a fully integrated server system directly from Intel using its online Configure-to-Order (CTO) tool. Or, the Advanced System Management product key can be purchased separately and installed later. When purchasing the product key separately from the system, instructions will be provided on where to register the product key with Intel. A license file is then downloaded onto the system where the Integrated BMC Web Console or the SYSCFG utility are used to upload the key to the BMC firmware to unlock the advanced features.

5.3.1 Virtual Media Image Redirection (HTML5 and Java)

The BMC supports media redirection of local folders and .IMG and .ISO image files. This redirection is supported in both HTML5 and Java remote console clients. When the user selects “Virtual Media over HTML5”, a new web page will be displayed that provides the user interface to select which type of source media (image file or file folder*) to mount, and then allows the user to select the desired media to make available to the server system. After the type and specific media are selected, the interface provides a mount/unmount interface so the user can connect the media to or disconnect the media from the server system. Once connected, the selected image file or file folder is presented in the server system as standard

removable media and may be interacted within the normal fashion based on the operating system running on the server system. This feature allows system administrators the ability to install software (including operating system installation), copy files, perform firmware updates, and so on from media on their remote workstation.

Note: The file folder share is presented to the server system as a UDF file system; the server system operating system must be able to interact with UDF file systems for this feature to be used with the operating system.

5.3.2 Virtual Media over network share and local folder

In addition to supporting virtual media redirection from the remote workstation (see Section 5.3.1), the BMC also supports media redirection of file folders and .IMG and .ISO files hosted on a network file server accessible to the BMC network interface. The current version supports Samba shares (Microsoft* Windows* file shares). Future versions will add support for NFS shares. This virtual media redirection is more effective for mounting virtual media at scale, instead of processing all files from the workstation's drive through the HTML5 application and over the workstation's network. Each BMC makes a direct network file share connection to the file server and accesses files across that network share directly.

5.3.3 Active Directory support

The BMC supports Active Directory. Active Directory (AD) is a directory service developed by Microsoft* for Windows domain networks. This feature allows users to login to the web console or Redfish* using an active directory username instead of local authentication. The feature allows administrators to only change passwords on this single domain account instead on every remote system.

5.4 Intel® Data Center Manager (DCM) Support

Intel® DCM is a solution for out-of-band monitoring and managing the health, power, and thermals of servers and a variety of other types of devices.

What can you do with Intel® DCM?

- Automate health monitoring
- Improve system manageability
- Simplify capacity planning
- Identify underutilized servers
- Measure energy use by device
- Pinpoint power/thermal issues
- Create power-aware job scheduling tasks
- Increase rack densities
- Set power policies and caps
- Improve data center thermal profile
- Optimize application power consumption
- Avoid expensive PDUs and smart power strips

For more information, go to

https://www.intel.com/content/www/us/en/software/intel-dcm-product-detail.html

6. Server Board Connector / Header Pinout Definition

This chapter identifies the location and pinout for most server board connectors and headers on the server board. Information for some connectors and headers is found elsewhere in the document where the feature is described in more detail.

Pinout definition for the following server board connectors is only made available by obtaining the board schematics directly from Intel (NDA required).

- All riser slots
- OCP* module mezzanine connector
- M.2 SSD connectors
- DIMM slots
- Processor sockets

Note: See Appendix F for a list of connectors / headers used on the server board. The appendix provides a list of manufacturers and part numbers.

6.1 Power Connectors

The server board includes several power connectors that are used to provide DC power to various devices.

6.1.1 Main Power Connectors

Main server board power is supplied from two slot connectors that allow support for one or two CRPS type power supplies to dock directly to the server board. The connectors are labeled “MAIN PWR 1” and “MAIN PWR 2” on the server board as shown in the following figure. The server board provides no option to support power supplies with cable harnesses. In a redundant power supply configuration, a failed power supply module is hot-swappable. Table 14 provides the pinout for the “MAIN PWR 1” and “MAIN PWR 2” connectors. The connector manufacturer is Amphenol* ICC (FCI); manufacturer part number is 10035388-102LF.

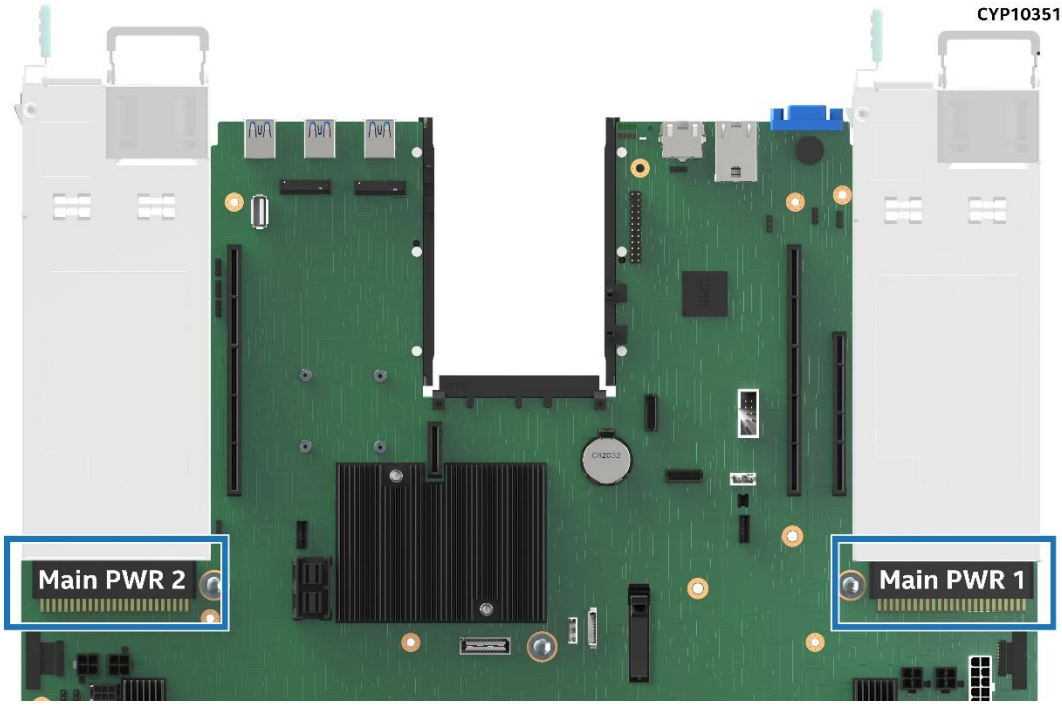


Figure 32. “MAIN PWR 1” and “MAIN PWR 2” Connectors

Table 14. Main Power (Slot 1) and Main Power (Slot 2) Connector Pinout ("MAIN PWR 1" and "MAIN PWR 2")

Pin #	Signal Name	Pin #	Signal Name
B1	GROUND	**A1**	GROUND
B2	GROUND	**A2**	GROUND
B3	GROUND	**A3**	GROUND
B4	GROUND	**A4**	GROUND
B5	GROUND	**A5**	GROUND
B6	GROUND	**A6**	GROUND
B7	GROUND	**A7**	GROUND
B8	GROUND	**A8**	GROUND
B9	GROUND	**A9**	GROUND
B10	P12V	**A10**	P12V
B11	P12V	**A11**	P12V
B12	P12V	**A12**	P12V
B13	P12V	**A13**	P12V
B14	P12V	**A14**	P12V
B15	P12V	**A15**	P12V
B16	P12V	**A16**	P12V
B17	P12V	**A17**	P12V
B18	P12V	**A18**	P12V
B19	P3V3_AUX: PD_PS1_FRU_A0	**A19**	SMB_PMBUS_DATA_R
B20	P3V3_AUX: PD_PS1_FRU_A1	**A20**	SMB_PMBUS_CLK_R
B21	P12V_STBY	**A21**	FM_PS_EN_PSU_N
B22	FM_PS_CR1	**A22**	IRQ_SML1_PMBUS_ALERTR2_N
B23	P12V_SHARE	**A23**	ISENSE_P12V_SENSE_RTN
B24	TP_1_B24 (for MAIN PWR 1) TP_2_B24 (for "MAIN PWR 2)	**A24**	ISENSE_P12V_SENSE
B25	FM_PS_COMPATIBILITY_BUS	**A25**	PWRGD_PS_PWROK

6.1.2 Hot Swap Backplane Power Connector

The server board includes one white 2x6-pin power connector that, when cabled, provides power for hot swap backplanes, as shown in Figure 33. On the server board, this connector is labeled "HSBP PWR". The connector manufacturer is Foxconn Interconnect Technology Limited; manufacturer part number is HM3506E-HP1.

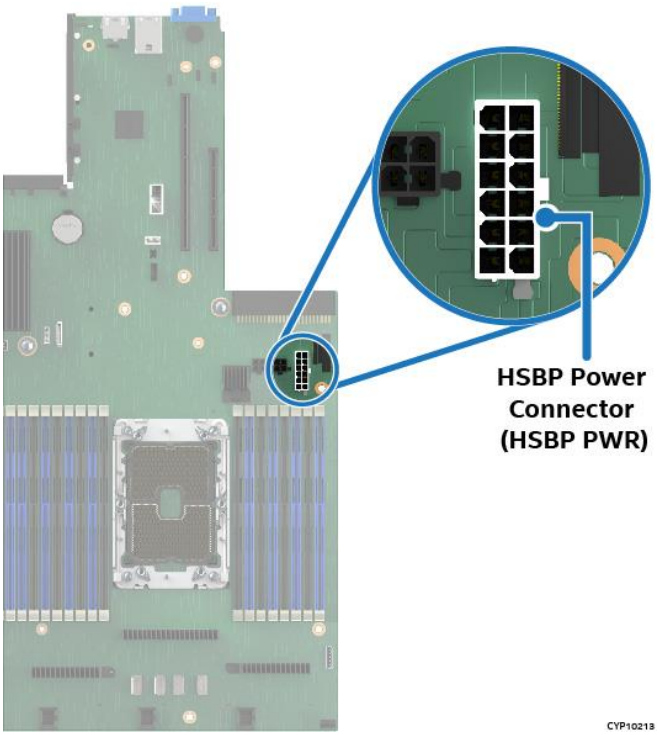


Figure 33. Hot Swap Backplane Power Connector

Table 15. Hot Swap Backplane Power Connector Pinout (“HSBP PWR”)

Pin #	Signal Name	Pin #	Signal Name
1	GND	7	P12V_240VA3
2	GND	8	P12V_240VA3
3	GND	9	P12V_240VA2
4	GND	10	P12V_240VA2
5	GND	11	P12V_240VA1
6	GND	12	P12V_240VA1

6.1.3 Optional 12-V Power Connectors

The server board includes five 2x2-pin power connectors labeled “OPT_12V_PWR”. The connectors provide supplemental 12 V power-out to high-power PCIe* x16 add-in cards that have power requirements that exceed the 75 W maximum power supplied by the riser card slot. These connectors are identified in the following figure. A cable from the connectors may be routed to a power-in connector on the given add-in card. Maximum power draw for each connector is 225 W. Maximum power is also limited by available power provided by the power supply and the total power draw of the given system configuration. A power budget calculation for the complete system should be performed to determine how much supplemental power is available to support any high-power add-in cards. The connector manufacturer is Foxconn* Interconnect Technology Limited; manufacturer part number is HM3502E-HS7.

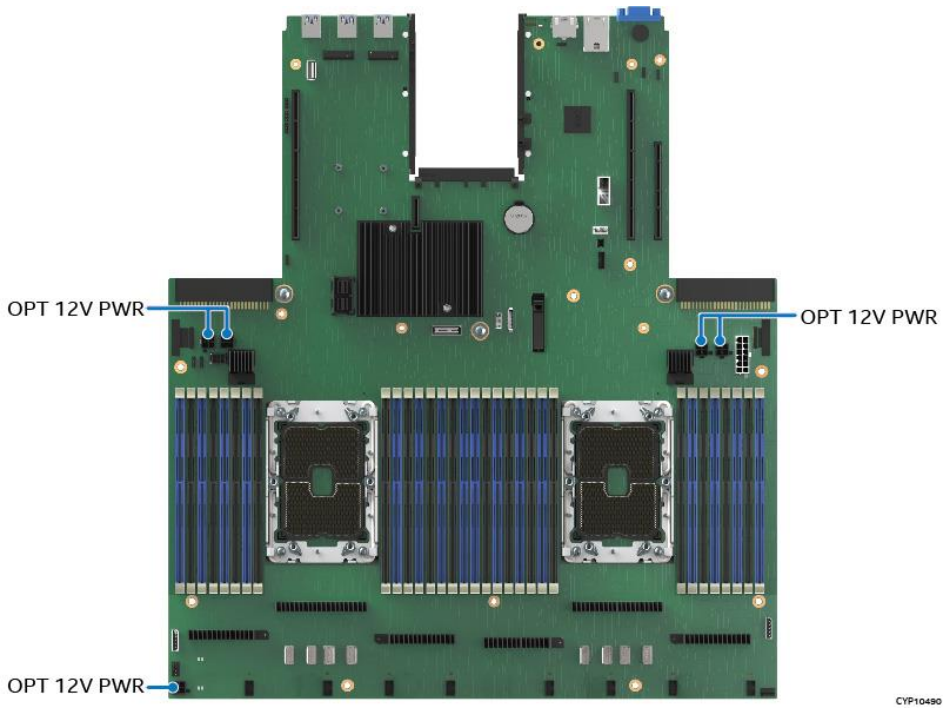


Figure 34. Riser Slot Auxiliary Power Connectors

The following table provides the pinout of the 12-V power connectors.

Table 16. Riser Slot Auxiliary Power Connector Pinout

Pin #	Signal Name
1	GROUND
2	GROUND
3	P12V
4	P12V

6.1.4 Peripheral Power Connector

The server board includes one 6-pin power connector intended to provide power for peripheral devices such as solid state devices (SSDs). The power connector supports 3.3, 5, 12 volts. On the server board, this connector is labeled “Peripheral_ PWR”. The following table provides the pinout for this connector. The connector manufacturer is Foxconn Interconnect Technology Limited; manufacturer part number is HM3502E-HS7.

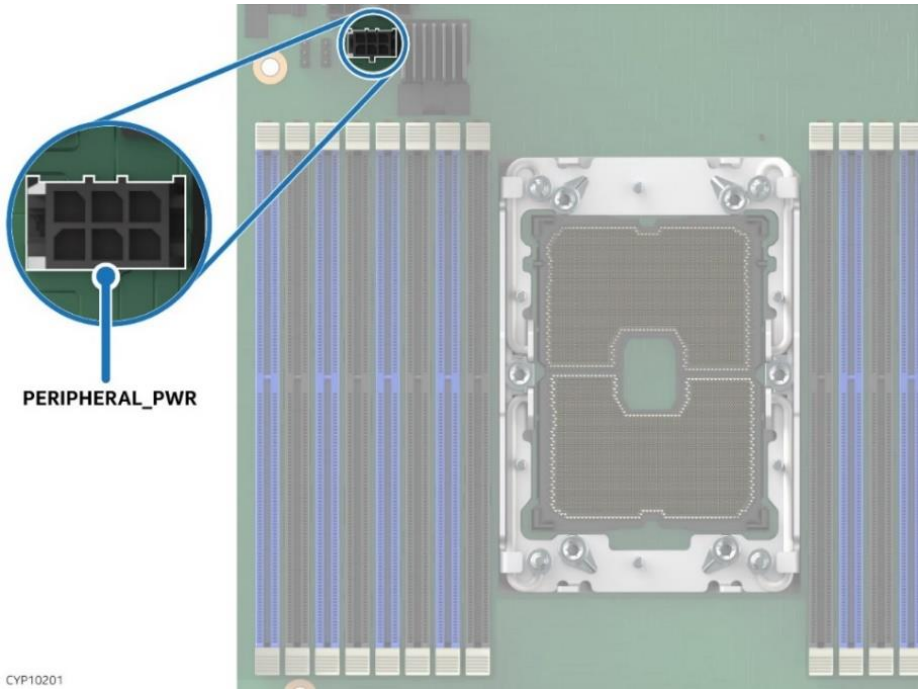


Figure 35. Peripheral Power Connector

Table 17. Peripheral Drive Power Connector Pinout

Pin #	Signal Name
1	P5V
2	P5V
3	GROUND
4	P12V
5	P3V3
6	GROUND

6.2 Front USB 3.0/2.0 Panel Header and Front Control Panel Header

The server board includes two headers that provide various front panel options. This section provides the pinout for each header. The headers shown in the figure are the same type. The header manufacturer is Hirose Electric* Company (U.S.A.) Incorporated; manufacturer part number is FH34SRJ-26S-0.5SH.

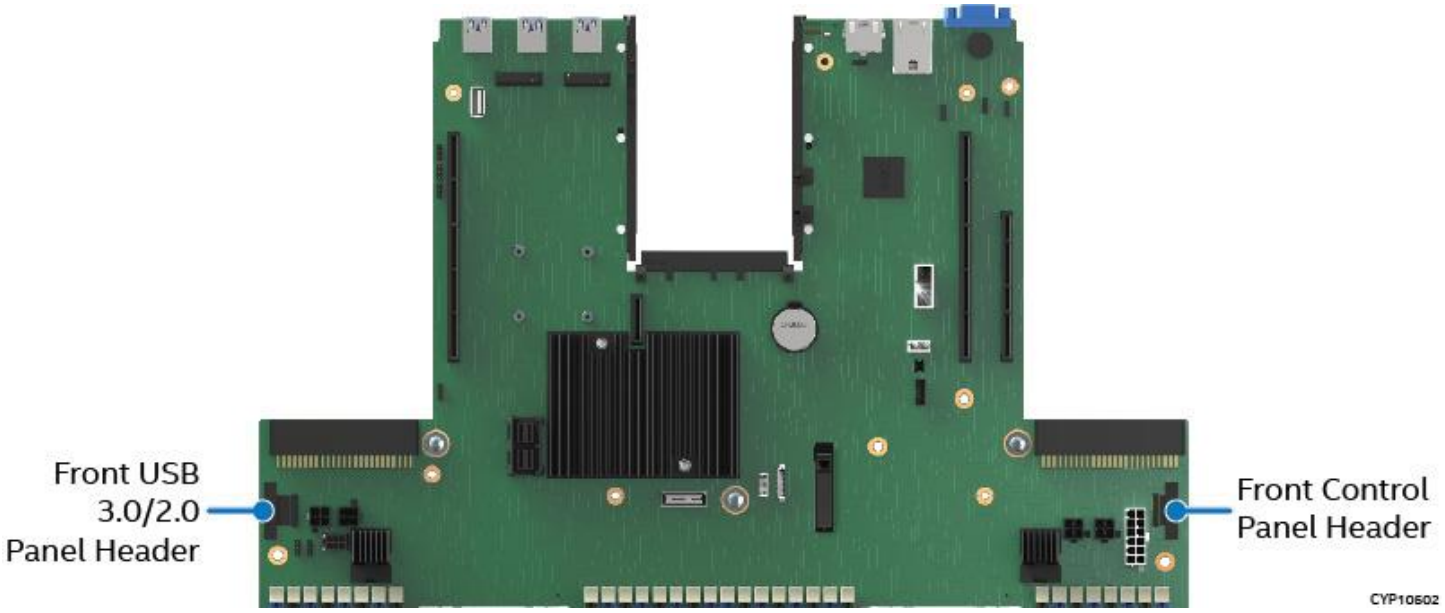


Figure 36. Front Panel Header and Front Control Panel Header

6.2.1 Front USB 3.0/2.0 Panel Header

The Front USB 3.0/2.0 Panel header is 26-pins. The following table provides the pinout.

Table 18. Front USB 3.0/2.0 Panel Header Pinout

Pin #	Signal Name	Pin #	Signal Name
1	P5V_USB3_FP	14	Ground
2	P5V_USB3_FP	15	USB3_BUFF_P01_RXN
3	P5V_USB3_FP	16	USB3_BUFF_P01_RXP
4	P5V_USB3_FP	17	Ground
5	P5V_USB3_FP	18	USB3_BUFF_P01_TXN
6	P5V_USB3_FP	19	USB3_BUFF_P01_TXP
7	P5V_FB_SB	20	Ground
8	Ground	21	USB2_BUFF_P11_DN
9	Ground	22	USB2_BUFF_P11_DP
10	Ground	23	Ground
11	Ground	24	USB2_BUFF_P13_DN
12	Ground	25	USB2_BUFF_P13_DP
13	Ground	26	Ground

6.2.2 Front Control Panel Header Pinout

The Front Control Panel header is 26 pins. The following table provides the pinout.

Table 19. Front Control Panel Header Pinout

Pin #	Signal Name	Pin #	Signal Name
1	GND	14	GND
2	GND	15	NIC1_SPEED_LED _N
3	NIC2_LINK_ACT_LED _N	16	PWR_BTN_N
4	NIC2_SPEED_LED _N	17	HDD_ACT_N
5	NMI_BTN_N	18	STATUS_LED_A_N
6	SPARE	19	STATUS_LED_G_N
7	CHASSIS_INTRUSSION	20	P3V3
8	ID_BTN_N	21	ID_LED_N
9	GND	22	PWR_LED_N
10	SMB_SCL	23	P5V_AUX
11	SMB_SDA	24	SPARE
12	RST_BTN_N	25	P3V3_AUX
13	NIC1_LINK_ACT_LED_N	26	P3V3_AUX

6.3 Serial Port B Header

Serial Port B is provided through an internal DH-10 header labeled “Serial_B” on the server board. This header adheres to the DTK pinout specification. The header location is shown in Figure 37 and the pinout is provided in Table 20. The Serial Port B header manufacturer is Wieson* Technologies Co., LTD; manufacturer part number is G2120C888-019H.

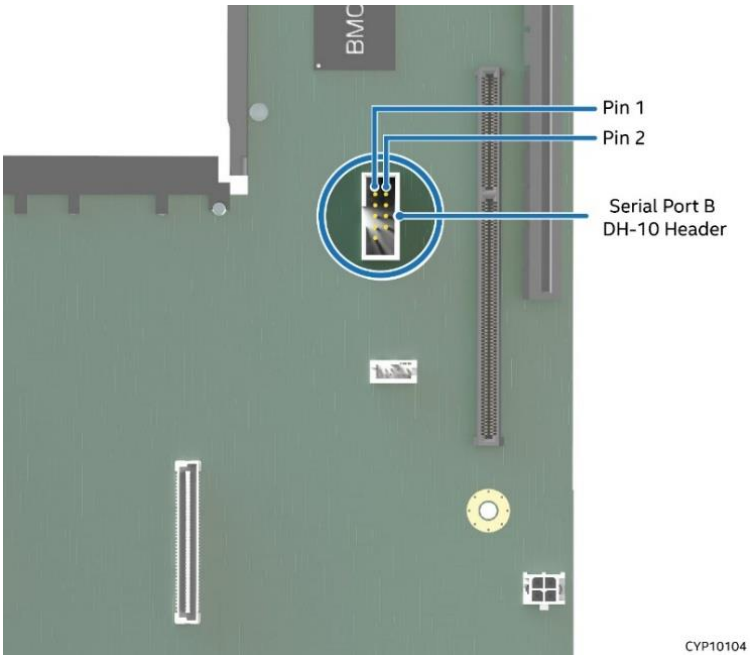


Figure 37. Serial Port B Header (internal)

Table 20. Serial Port B Header Pinout

Pin#	Signal Name	Pin#	Signal Name
1	DCD	**2**	DSR
3	SIN	**4**	RTS
5	SOUT	**6**	CTS
7	DTR	**8**	RI
9	GROUND		KEY

6.4 I²C Connectors

The server board contains two I²C connectors. The header locations are shown in Figure 38 and the pinout is provided in Table 21. The I²C header manufacturer is Wieson* Technologies company, LTD manufacturer part number is A2506WV-05P.

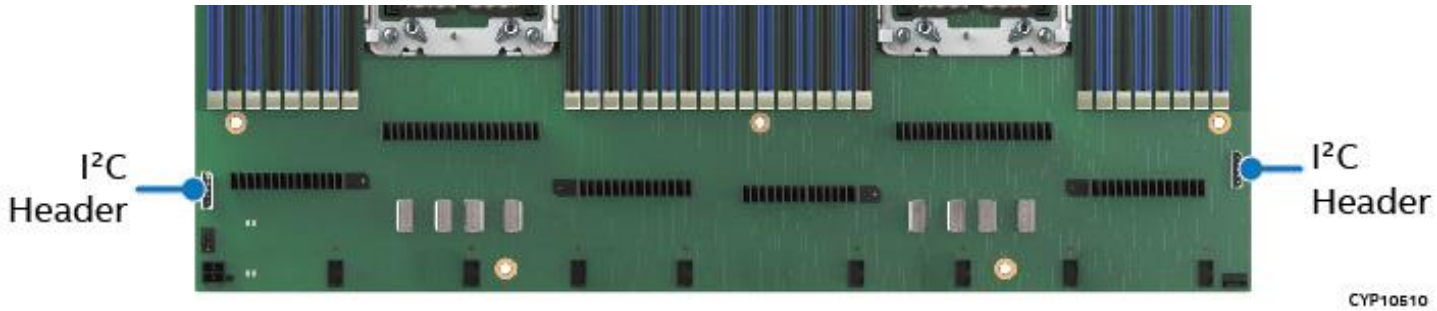


Figure 38. I²C Connectors

Table 21. I²C cable Connector Pinout

Pin #	Signal Name
1	SMB_3V3_DAT
2	GND
3	SMB_3V3_CLK
4	SMB_ADD0
5	SMB_ADD1

6.5 Fan Connectors

This section provides pinouts for the system fan connectors and CPU fan connectors.

6.5.1 System Fan Connectors

The Intel® Server Board M50CYP2SB1U and M50CYP2SBSTD have eight 8-pin fan connectors labeled "SYS_FAN #", where # is 1 through 8. The maximum power drawn by each 8-pin fan connector is 70 W. The 8-pin fan connector manufacturer is Foxconn Interconnect Technology Limited; manufacturer part number is HLH2047-LF00D-4H. The following figure and table show the pinout of the 8-pin fan connector.

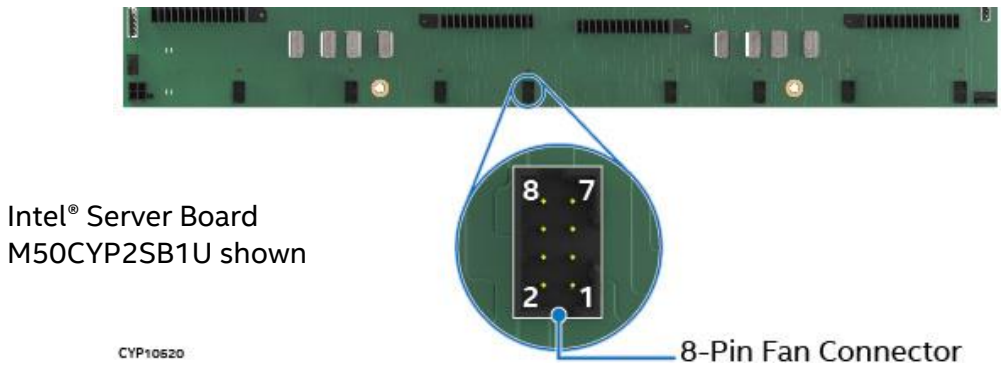


Figure 39. 8-Pin Fan Connector – Intel® Server Board M50CYP2SBSTD and M50CYP2SB1U

Table 22. 8-Pin Fan Connector Pinout – Intel® Server Board M50CYP2SBSTD and M50CYP2SB1U

Pin #	Signal Name	Pin #	Signal Name
8	FAN PRSNT	**7**	GROUND
6	GROUND	**5**	Fan Tachometer 1 (Sense)
4	P12V FAN	**3**	P12V FAN
2	FAN PWM	**1**	Fan Tachometer 2 (Sense)

In addition to the fan connectors shown above, the Intel® Server Board M50CYP2SBSTD has six 6-pin fan connectors labeled "SYS_FAN #", where # is 1 through 6. The maximum power drawn by each 6-pin fan connector is 50.4 W. The 6-pin fan connector manufacturer is Lotes Company; manufacturer part number is ABA-WAF-050-Y37. The following figure and table show the pinout of the 6-pin fan connector.

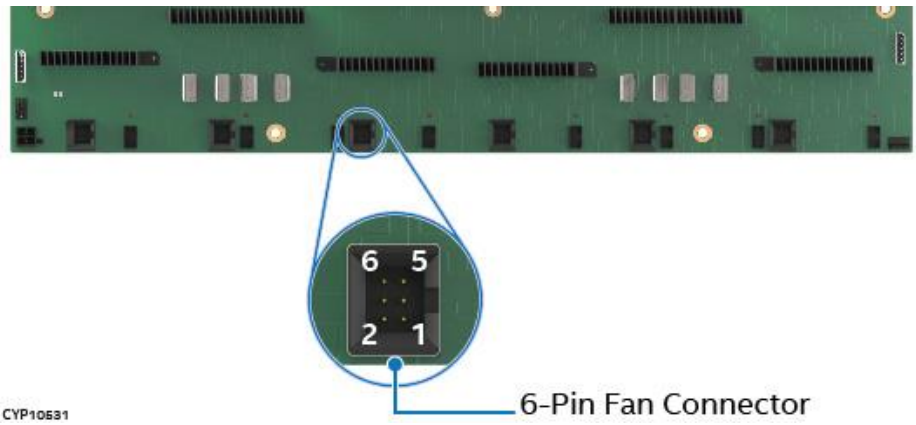


Figure 40. 6-Pin Fan Connector – Intel® Server Board M50CYP2SBSTD

Table 23. 6-Pin Fan Pinout – Intel® Server Board M50CYP2SBSTD

Pin #	Signal Name	Pin #	Signal Name
6	LED FAN FAULT	**5**	SYS FAN PRSNT
4	FAN PWM	**3**	FAN TACH
2	P12V FAN	**1**	GROUND

6.5.2 CPU Fan Connectors

The server board has two 4-pin CPU fan connectors: one for CPU 0 and one for CPU 1. The connector manufacturer is Foxconn Interconnect Technology Limited; manufacturer part number is HF2704E-M1.

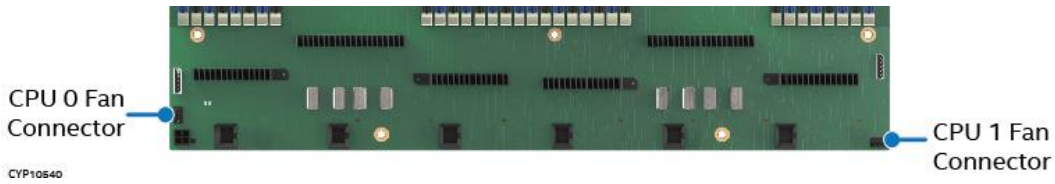


Figure 41. CPU 0 / CPU 1 Fan Connectors

Table 24. CPU 0 / CPU 1 Fan Pinout

Pin #	Signal Name
1	GND
2	12V
3	Tach/Sense
4	PWM (Control)

6.6 PCIe* SlimSAS* Connector

To provide support for PCIe NVMe SSDs, the server board includes eight PCIe SlimSAS connectors. PCIe lanes from each CPU are routed to a bank of four connectors labeled “CPU 0 PCIe Ports A-D” and “CPU1 PCIe Ports A-D”. Each SlimSAS connector supports x4 PCIe lanes. The following tables provide the pinout for each PCIe* SlimSAS connector. The connector manufacturer is Amphenol* ICC (FCI); manufacturer part number is U10DH3825002T.

Figure 42. PCIe* SlimSAS* Connectors

Table 25. PCIe* SlimSAS* Connector A Pinout (CPU 0 and CPU 1)

Pin #	Signal Name	Pin #	Signal Name
A1	GND	**B1**	GND
A2	PERp<0>	**B2**	PETp<0>
A3	PERn<0>	**B3**	PETn<0>
A4	GND	**B4**	GND
A5	PERp<1>	**B5**	PETp<1>
A6	PERn<1>	**B6**	PETn<1>
A7	GND	**B7**	GND
A8	BP_TYPE	**B8**	HP_SMB_CLK
A9	SSD_ID0	**B9**	HP_SMB_DAT
A10	GND	**B10**	GND
A11	CLK_100M_P	**B11**	PE_RST#
A12	CLK_100M_N	**B12**	SSD0_PRSNT_N
A13	GND	**B13**	GND
A14	PERp<2>	**B14**	PETp<2>
A15	PERn<2>	**B15**	PETn<2>
A16	GND	**B16**	GND
A17	PERp<3>	**B17**	PETp<3>
A18	PERn<3>	**B18**	PETn<3>
A19	GND	**B19**	GND

Table 26. PCIe* SlimSAS* Connector B Pinout (CPU 0 and CPU 1)

Pin #	Signal Name	Pin #	Signal Name
A1	GND	**B1**	GND
A2	PERp<4>	**B2**	PETp<4>
A3	PERn<4>	**B3**	PETn<4>
A4	GND	**B4**	GND
A5	PERp<5>	**B5**	PETp<5>
A6	PERn<5>	**B6**	PETn<5>
A7	GND	**B7**	GND
A8	BP_TYPE	**B8**	SMB_ALERT_N
A9	SSD_ID1	**B9**	CPU 0: FM_SASM_CPU0_N CPU 1: RSVD
A10	GND	**B10**	GND
A11	CLK_100M_P	**B11**	PE_RST#
A12	CLK_100M_N	**B12**	SSD1_PRSNT_N
A13	GND	**B13**	GND
A14	PERp<6>	**B14**	PETp<6>
A15	PERn<6>	**B15**	PETn<6>
A16	GND	**B16**	GND
A17	PERp<7>	**B17**	PETp<7>
A18	PERn<7>	**B18**	PETn<7>
A19	GND	**B19**	GND

Table 27. PCIe* SlimSAS* Connector C Pinout (CPU 0 and CPU 1)

Pin #	Signal Name	Pin #	Signal Name
A1	GND	**B1**	GND
A2	PERp<0>	**B2**	PETp<0>
A3	PERn<0>	**B3**	PETn<0>
A4	GND	**B4**	GND
A5	PERp<1>	**B5**	PETp<1>
A6	PERn<1>	**B6**	PETn<1>
A7	GND	**B7**	GND
A8	BP_TYPE	**B8**	HP_SMB_CLK
A9	SSD_ID2	**B9**	HP_SMB_DAT
A10	GND	**B10**	GND
A11	CLK_100M_P	**B11**	PE_RST#
A12	CLK_100M_N	**B12**	SSD2_PRSNT_N
A13	GND	**B13**	GND
A14	PERp<2>	**B14**	PETp<2>
A15	PERn<2>	**B15**	PETn<2>
A16	GND	**B16**	GND
A17	PERp<3>	**B17**	PETp<3>
A18	PERn<3>	**B18**	PETn<3>
A19	GND	**B19**	GND

Table 28. PCIe* SlimSAS* Connector D Pinout (CPU 0 and CPU 1)

Pin #	Signal Name	Pin #	Signal Name
A1	GND	**B1**	GND
A2	PERp<4>	**B2**	PETp<4>
A3	PERn<4>	**B3**	PETn<4>
A4	GND	**B4**	GND
A5	PERp<5>	**B5**	PETp<5>
A6	PERn<5>	**B6**	PETn<5>
A7	GND	**B7**	GND
A8	BP_TYPE	**B8**	SMB_ALERT_N
A9	SSD_ID3	**B9**	CPU 0: RSVD CPU 1: FM_SASM_CPU1_N
A10	GND	**B10**	GND
A11	CLK_100M_P	**B11**	PE_RST#
A12	CLK_100M_N	**B12**	SSD3_PRSNT_N
A13	GND	**B13**	GND
A14	PERp<6>	**B14**	PETp<6>
A15	PERn<6>	**B15**	PETn<6>
A16	GND	**B16**	GND
A17	PERp<7>	**B17**	PETp<7>
A18	PERn<7>	**B18**	PETn<7>
A19	GND	**B19**	GND

7. PCI Express (PCIe*) Support

This chapter provides information on the Intel® Server Board M50CYP2SB family PCI Express (PCIe*) support. The PCIe* interfaces supporting riser slots and server board PCIe* SlimSAS connectors are fully compliant with the *PCIe* Base Specification, Revision 4.0* supporting the following PCIe* bit rates: 4.0 (16 GT/s), 3.0 (8.0 GT/s), 2.0 (5.0 GT/s), and 1.0 (2.5 GT/s).

The following table provides the processor/chipset port routing for PCIe-based server board connectors including OCP* connector, PCIe* SlimSAS* connectors, and riser card slots. The interfaces supporting M2 connectors are fully compliant with the *PCIe* Base Specification, Revision 3.0* supporting the following PCIe* bit rates: 3.0 (8.0 GT/s), 2.0 (5.0 GT/s), and 1.0 (2.5 GT/s).

Table 29. Processor / Chipset PCIe* Port Routing

Host	Port	Width	Gen.	Usage
CPU 0	Port 0A–0D	x16	4.0	OCP* Adapter Mezzanine connector
	Port 1A–1D	x16	4.0	Riser Slot #1 [15:0]
	Port 2A–2D	x16	4.0	Riser Slot #1 [31:16]
	Port 3A–3D	x16	4.0	Server board PCIe* SlimSAS connectors
	DMI3	x4	3.0	Chipset (PCH)
CPU 1	Port 0A–0D	x16	4.0	Riser Slot #3 [15:0]
	Port 1A–1D	x16	4.0	Riser Slot #2 [31:16]
	Port 2A–2D	x16	4.0	Riser Slot #2 [15:0]
	Port 3A–3D	x16	4.0	Server board PCIe* SlimSAS connectors
Chipset (PCH)	Port 4–7	x4	3.0	M.2 Connector- SATA / PCIe*
	Port 8–11	x4	3.0	M.2 Connector- SATA / PCIe*

7.1 PCIe* Enumeration and Allocation

The BIOS assigns PCI bus numbers in a depth-first hierarchy, in accordance with the *PCIe* Local Specification, Revision 4.0*. The bus number is incremented when the BIOS encounters a PCI-PCI bridge device.

Scanning continues on the secondary side of the bridge until all subordinate buses are assigned numbers. PCI bus number assignments may vary from boot to boot with varying presence of PCI devices with PCI-PCI bridges.

If a bridge device with a single bus behind it is inserted into a PCIe* bus, all subsequent PCIe* bus numbers below the current bus are increased by one. The bus assignments occur once, early in the BIOS boot process, and never change during the pre-boot phase.

7.2 PCIe* Riser Card Support

The server board provides three riser card slots identified as: Riser Slot #1, Riser Slot #2, and Riser Slot #3. The PCIe* bus lanes for Riser Slot #1 are supported by CPU 0. The PCIe* bus lanes for Riser Slot #2 and Riser Slot #3 are supported by CPU 1.

Note: The riser card slots are specifically designed to support riser cards only. Attempting to install a PCIe* add-in card directly into a riser card slot on the server board may damage the server board, the add-in card, or both.

Note: A dual processor configuration is required when using Riser Slot #2 and Riser Slot #3.

7.3 PCIe* Interposer Riser Slot (Intel® Server Board M50CYP2SB1U Only)

The PCIe* Interposer Riser Slot and PCIe* interposer riser card were designed to provide additional add-in card support for the server system. The PCIe* interposer riser card shown in the following figure is an accessory option supported by the PCIe* Interposer Riser Slot.

This card has one PCIe* add-in card slot (x8 electrical, x8 mechanical) labeled “Slot1_PCIe_x8” that supports one low profile, half length, single-width add-in card.

The PCIe* interposer riser card also has one x8 PCIe* NVMe* SlimSAS* connector labeled “Slot1_PCIe_AIC_Interposer”.

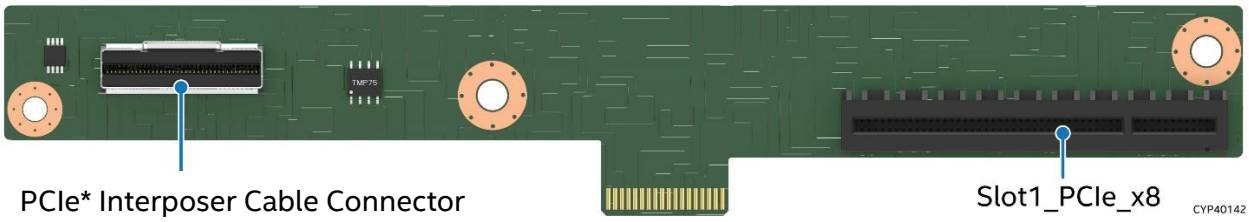


Figure 43. PCIe* Interposer Riser Card

Table 30. PCIe* Interposer Riser Card Connector Description

Connector	Description
Slot1_PCIe_x8	CPU 1 – Ports 1A through 1B (x8 electrical, x8 mechanical)
PCIe* Interposer Cable Connector	CPU 1 – Ports 1A through 1B (x8 electrical, x8 mechanical)

Table 31. PCIe* Interposer Riser Slot Pinout

Pin #	PCIe* Signal (from processor perspective)	Pin #	PCIe* Signal (from processor perspective)
A1	GND	**B1**	GND
A2	Spare	**B2**	Spare
A3	Spare	**B3**	Spare
A4	GND	**B4**	GND
A5	12V	**B5**	12V
A6	12V	**B6**	12V
A7	GND	**B7**	GND

Pin #	PCIe* Signal (from processor perspective)	Pin #	PCIe* Signal (from processor perspective)
A8	12V	**B8**	12V
A9	12V	**B9**	12V
A10	GND	**B10**	GND
A11	3.3VAUX	**B11**	Spare
A12	3.3V PWRGD	**B12**	Spare
A13	GND	**B13**	GND
A14	SMBus Clock	**B14**	Spare
A15	SMBus Data	**B15**	Spare
A16	GND	**B16**	GND
A17	FRU/Temp ADDR [I]	**B17**	PERST_N
A18	PWRBRK_N	**B18**	PE_WAKE_N
A19	GND	**B19**	GND
A20	REFCLK_TOP_P	**B20**	Riser ID[0]
A21	REFCLK_TOP_N	**B21**	Riser ID[1]
A22	GND	**B22**	GND
A23	Spare	**B23**	SYS_THROTTLE_N
A24	Spare	**B24**	MUX_RST_N
A25	GND	**B25**	GND
A26	Spare	**B26**	Spare
A27	Spare	**B27**	Spare
A28	GND	**B28**	GND

7.3.1 PCIe* Interposer Riser Card Usage in an Intel® Server System M50CYP1UR Family

The PCIe Interposer card's functionality depends on the PCIe* NVMe* riser card in Riser Slot #2. The x8 PCIe* data lanes used by the PCIe* add-in card slot are routed by an interface cable from Intel PCIe* NVMe* riser card (accessory option) plugged into Riser Slot #2. To use the interposer card, the PCIe* NVMe* SlimSAS connector on the PCIe* interposer riser card must be connected to the PCIe* NVMe* SlimSAS connector (PCIe_SSD_0-1) on the NVMe* riser card using the PCIe* interposer cable. The Intel accessory kit CYP1URISER2KIT includes:

- PCIe* interposer riser card
- PCIe* NVMe* riser card
- PCIe* interposer cable

Figure 44. PCIe* NVMe* Riser Card for Riser Slot #2

Note: The PCIe_SSD_0–1 connector only supports the PCIe Interposer cable. This connector does not support front drive bay connectivity.

Table 32. PCIe* NVMe* Riser Card Connector Description

Connector	Description
Slot1_PCIe_x16	CPU 1 – Ports 2A through 2D (x16 electrical, x16 mechanical)
PCIe_SSD_0-1	CPU 1 – Ports 1A through 1B (x8 electrical, x8 mechanical)

Note: The PCIe Interposer cable must not be completely inserted into the cable clip to ensure the cable does not pull on the riser cards. Place the cable at the mouth of the clip as shown in the following figure.

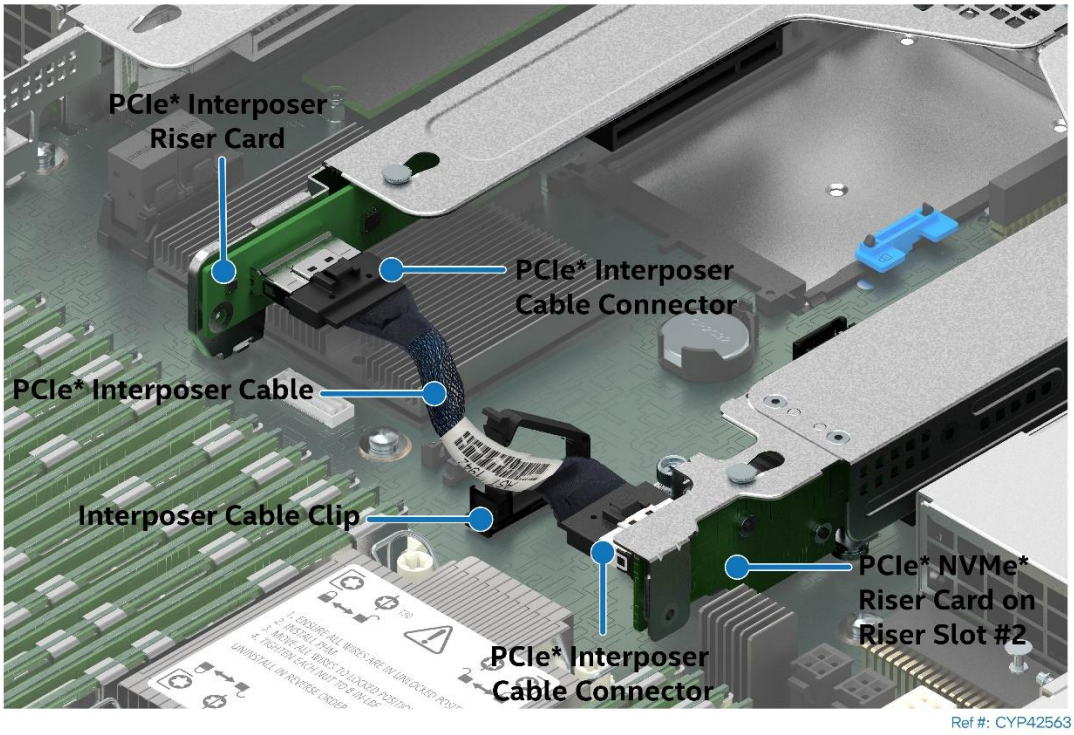


Figure 45. PCIe* Interposer Riser Card to PCIe* NVMe* Riser Card Connectivity

8. Storage Support

The Intel® Server Board M50CYP2SB family provides storage options not available on previous server board generations.

The server board supports up to two server board mounted M.2 PCIe*/SATA SSDs. The server board Mini-SAS HD (SFF-8643) connectors provide SATA SSD storage support.

The server board also provides various Non-Volatile Memory Express (NVMe*) storage options. NVMe* is an optimized, high-performance scalable storage interface designed to address the needs of enterprise systems that use PCIe*-based solid-state storage, providing efficient access to non-volatile memory storage devices. The NVMe* technology allows Intel server boards to take advantage of the levels of parallelism possible in modern SSDs.

Additional Intel® VROC NVMe* and Intel® VROC SATA capabilities are available. The Intel® Server Boards support Intel® VROC 7.5.

Support for different storage options varies depending on the configuration and/or available accessory options installed. This chapter provides an overview of server board storage support.

8.1 Server Board SATA Support

The server board uses two chipset-embedded AHCI SATA controllers, identified as “SATA” and “sSATA”. The AHCI sSATA controller supports up to two 6 GB/s SATA III ports (sSATA 1 and sSATA 2) using two M.2 SSD connectors. The AHCI SATA controller supports up to eight 6 GB/s SATA III ports on the server board. The following table describes the SATA and sSATA feature support.

Table 33. SATA and sSATA Controller Feature Support

Feature	Description	AHCI Mode	RAID Mode Intel® VROC (SATA RAID)
Native Command Queuing (NCQ)	Allows the device to reorder commands for more efficient data transfers	Supported	Supported
Auto Activate for direct memory access (DMA)	Collapses a DMA Setup, then DMA Activate sequence into a DMA Setup only	Supported	Supported
Hot Plug Support (U.2 Drives Only)	Allows for device detection without power being applied and ability to connect and disconnect devices without prior notification to the system	Supported	Supported
Asynchronous Signal Recovery	Provides a recovery from a loss of signal or establishing communication after hot plug	Supported	Supported
6 Gb/s Transfer Rate	Capable of data transfers up to 6 Gb/s	Supported	Supported
ATAPI Asynchronous Notification	A mechanism for a device to send a notification to the host that the device requires attention	Supported	Supported
Host and Link Initiated Power Management	Capability for the host controller or device to request Partial and Slumber interface power states	Supported	Supported
Staggered Spin-Up	Enables the host the ability to spin up hard drives sequentially to prevent power load problems on boot	Supported	Supported
Command Completion Coalescing	Reduces interrupt and completion overhead by allowing a specified number of commands to complete and then generating an interrupt to process the commands	Supported	N/A

The SATA controller and the sSATA controller can be independently enabled to function in AHCI mode, enabled to function in RAID mode or disabled. These controllers can be independently configured through the BIOS Setup utility under the **Advanced > Mass Storage Controller Configuration** menu screen.

8.1.1 SATA Support Through Mini-SAS HD Connectors

The eight SATA ports on the server board are as follows:

- Four ports from the Mini-SAS HD (SFF-8643) connector labeled “SATA_0–3” on the server board
- Four ports from the Mini-SAS HD (SFF-8643) connector labeled “SATA_4–7” on the server board

The following figure shows the SATA (0–3) and SATA (4–7) connectors on the server board.

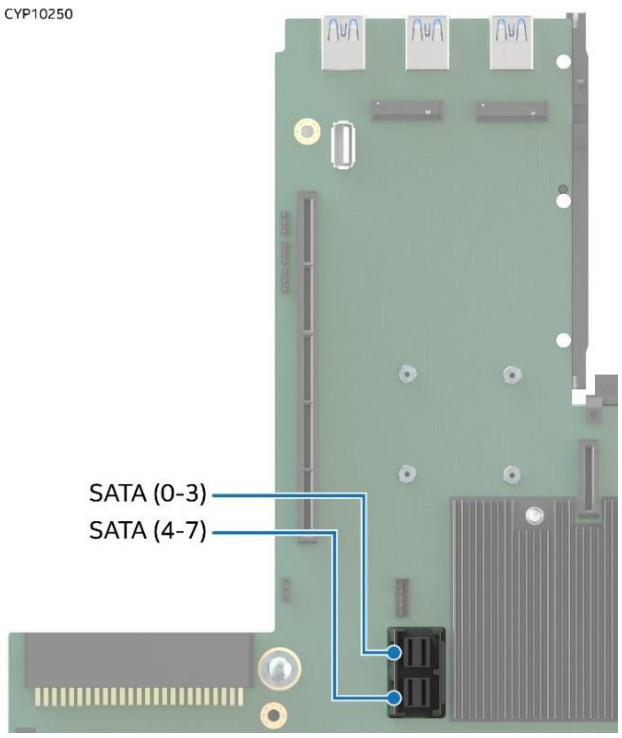


Figure 46. SATA Ports on Server Board

8.1.2 SATA Support Through M.2 Connectors

Refer to Section 8.2.

8.1.3 Staggered Disk Spin-Up

Because of the high density of disk drives that can be attached to the server board Intel® C621A chipset AHCI SATA controller and the sSATA controller, the combined startup power demand surge for all drives at once can be much higher than the normal running power requirements. This condition could require a much larger power supply for startup than for normal operations.

To mitigate this condition and lessen the peak power demand during system startup, both the AHCI SATA Controller and the sSATA Controller implement a Staggered Spin-Up capability for the attached drives. This means that the drives are started up separately, with a certain delay between disk drives starting.

For the server board SATA controller, staggered spin-up is an option – **AHCI HDD Staggered Spin-Up** – in the Mass Storage Controller Configuration screen found in the BIOS Setup utility.

8.2 M.2 SSD Storage Support

The server board includes two M.2 SSD connectors as shown in the following figure. The connectors are labeled “M2_x4PCIE/SSATA_1 (port 0)” and “M2_x4PCIE/SSATA_2 (port 1)” on the board. Each M.2 slot supports a PCIe* NVMe* or SATA drive that conforms to a 22110 (110 mm) or 2280 (80 mm) form factor.

Each M.2 slot is connected to four PCIe* lanes from the chipset’s embedded controller. The M.2 NVMe* drives can be combined into a VROC RAID volume.

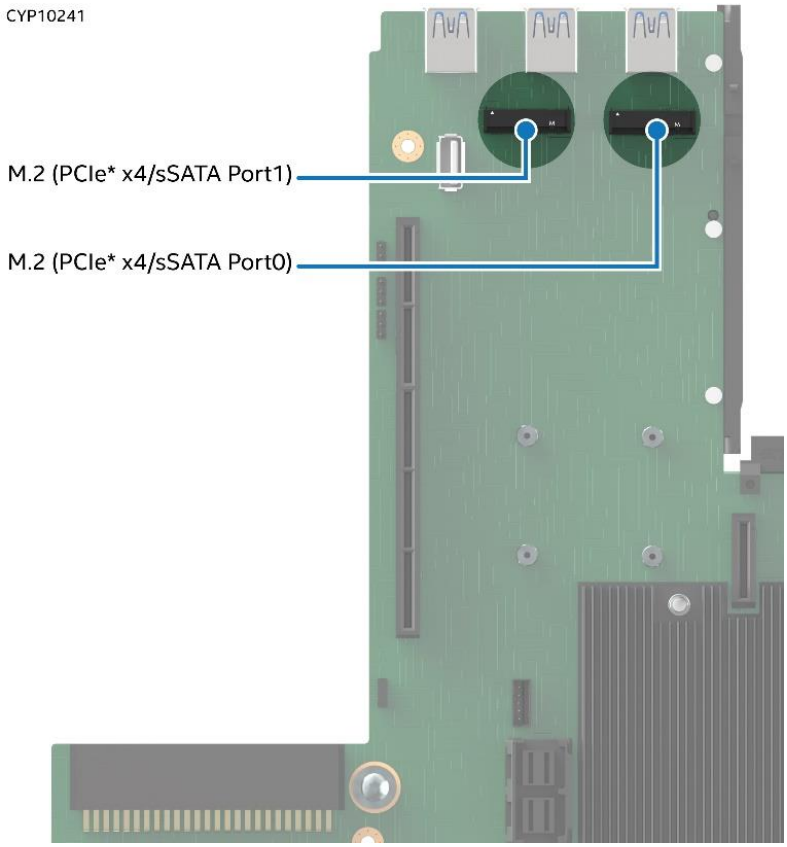


Figure 47. M.2 Module Connector Location

8.3 NVMe* Storage Support

Non-Volatile Memory Express (NVMe*) is an optimized, high-performance scalable storage interface designed to address the needs of enterprise systems that use PCIe®-based solid-state storage. NVMe* provides efficient access to non-volatile memory storage devices. The NVMe* technology allows Intel server boards to take advantage of the levels of parallelism possible in modern SSDs.

8.3.1 PCIe* SlimSAS* Support

SlimSAS* is a next generation ultra-high-speed interconnect solution for server boards and storage devices. They offer superior signal integrity performance over standard Mini-SAS HD connectors. The SlimSAS connectors are compliant with T10/Serial attached SCSI (SAS-4) standard.

The server board includes eight x4 PCIe* SlimSAS* connectors. These connectors can be used to connect the server board to NVMe* drives. PCIe* lanes from CPU 0 and CPU 1 are each routed to four PCIe* SlimSAS* connectors. See the following figure. The CPU 0 PCIe* SlimSAS* connectors are labeled “CPU0_PCIe*_PortA” through “CPU0_PCIe*_PortD” on the server board. The CPU 1 PCIe* SlimSAS* connectors are labeled “CPU1_PCIe*_PortA” through “CPU1_PCIe*_PortD” on the server board.

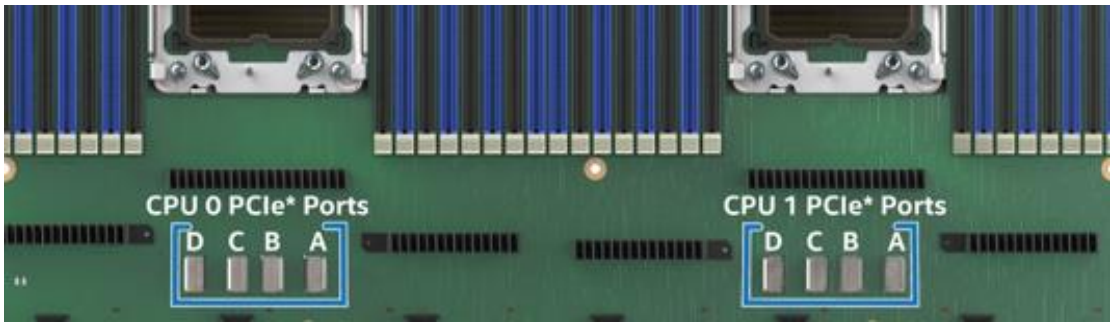


Figure 48. PCIe* SlimSAS* Connectors

The following table provides the PCIe* port routing information for the server board PCIe* SlimSAS connectors.

Table 34. CPU to PCIe* NVMe* SlimSAS* Connector Routing

Host	CPU Port	Routed to SlimSAS* Connector
CPU 0	Port 3A	CPU0_PCIe*_PortA
	Port 3B	CPU0_PCIe*_PortB
	Port 3C	CPU0_PCIe*_PortC
	Port 3D	CPU0_PCIe*_PortD
CPU 1	Port 3A	CPU1_PCIe*_PortA
	Port 3B	CPU0_PCIe*_PortB
	Port 3C	CPU1_PCIe*_PortC
	Port 3D	CPU0_PCIe*_PortD

8.3.2 Intel® Volume Management Device (Intel® VMD) 2.0 for NVMe*

Intel® Volume Management Device (Intel® VMD) is hardware logic inside the processor root complex to help manage PCIe* NVMe* SSDs. It provides robust hot plug support and status LED management. This allows servicing of storage system NVMe* SSD media without system crashes or hangs when ejecting or inserting NVMe* SSD devices on the PCIe* bus.

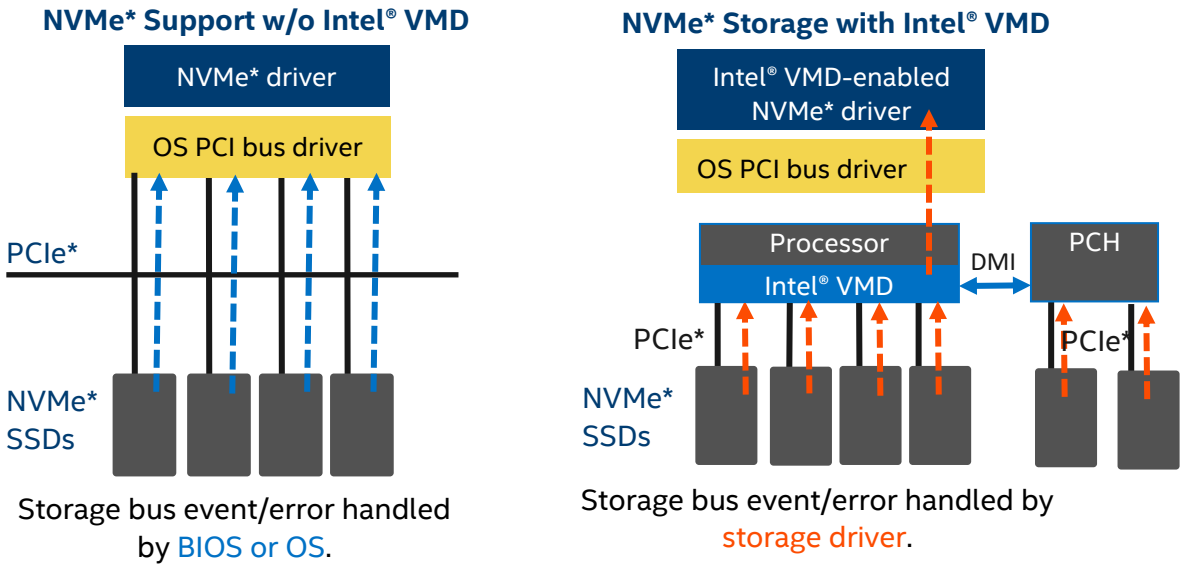


Figure 49. NVMe* Storage Bus Event / Error Handling

Intel® VMD handles the physical management of NVMe* storage devices as a stand-alone function but can be enhanced when Intel® Virtual RAID on CPU (Intel® VROC) support options are enabled to implement RAID based storage systems.

8.3.2.1 Intel® VMD 2.0 Features

Intel® VMD 2.0 includes the following features and capabilities:

- Hardware is integrated inside the processor PCIe* root complex.
- Entire PCIe* trees are mapped into their own address spaces (domains).
- Each domain manages x16 PCIe* lanes.
- Can be enabled/disabled in BIOS Setup at x4 lane granularity.
- Driver sets up/manages the domain (enumerate, event/error handling).
- May load an additional child device driver that is Intel® VMD aware.
- Hot plug support - hot insert array of PCIe* NVMe* SSDs.
- Support for PCIe* NVMe* SSDs only (no network interface controllers (NICs), graphics cards, and so on)
- Maximum of 128 PCIe* bus numbers per domain.
- Support for Management Component Transport Protocol (MCTP) over SMBus* only.
- Support for MMIO only (no port-mapped I/O).
- Does not support NTB, Quick Data Tech, Intel® Omni-Path Architecture (Intel® OPA), or SR-IOV.
- Correctable errors do not bring down the system.
- Intel® VMD only manages devices on PCIe* lanes routed directly from the processor or PCH chipset.
- When Intel® VMD is enabled, the BIOS does not enumerate devices that are behind Intel® VMD. The Intel® VMD-enabled driver is responsible for enumerating these devices and exposing them to the host.

8.3.2.2 Enabling Intel® VMD 2.0 for NVMe* Support

For installed NVMe* devices to use the Intel® VMD features in the system, Intel® VMD must be enabled on the appropriate processor PCIe* root ports in BIOS Setup. By default, Intel® VMD support is disabled on all processor PCIe* root ports in BIOS Setup.

The following table provides the PCIe* port routing information for the server board PCIe* SlimSAS connectors.

Table 35. CPU to PCIe* NVMe* SlimSAS* Connector Routing

Host	CPU Port	Routed to SlimSAS* Connector
CPU 0	Port 3A	CPU0_PCIe*_PortA
	Port 3B	CPU0_PCIe*_PortB
	Port 3C	CPU0_PCIe*_PortC
	Port 3D	CPU0_PCIe*_PortD
CPU 1	Port 3A	CPU1_PCIe*_PortA
	Port 3B	CPU0_PCIe*_PortB
	Port 3C	CPU1_PCIe*_PortC
	Port 3D	CPU0_PCIe*_PortD

In BIOS Setup, the Intel® VMD support menu is on the following menu tab: **Advanced** > **PCI Configuration** > **Volume Management Device.**

8.3.3 Intel® Virtual RAID on Chip (Intel® VROC) for NVMe*

Intel® VROC 7.5 supports the following:

- I/O processor with controller (ROC) and DRAM.
- Protected write back cache – software and hardware that allows recovery from a double fault.
- Isolated storage devices from operating system for error handling.
- Protected R5 data from operating system crash.
- NVMe* SSD hot plug and surprise removal on processor PCIe* lanes.
- LED management for PCIe* attached storage.
- RAID/storage management using Representational State Transfer (RESTful) application programming interfaces (APIs).
- Graphical user interface (GUI) for Linux*.
- 4K native NVMe* SSD support.

Enabling Intel® VROC 7.5 support requires installation of an optional upgrade key on the server board as shown in Figure 50. Table 36 identifies available Intel® VROC 7.5 upgrade key options.

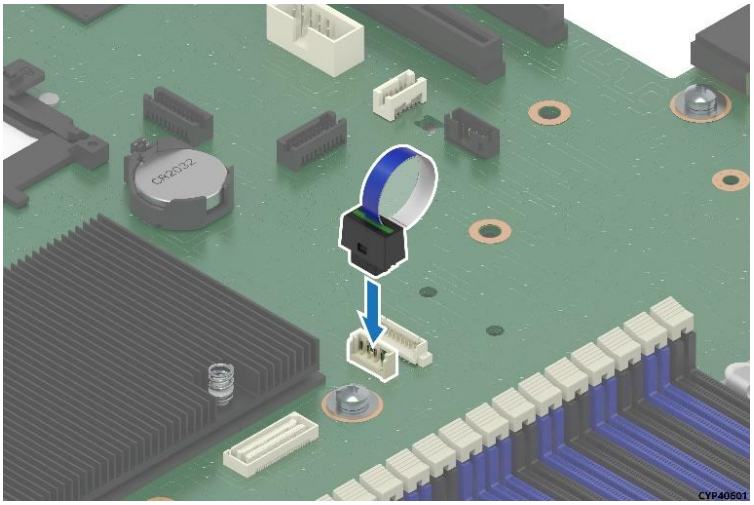


Figure 50. Intel® VROC 7.5 Key Insertion

Table 36. Optional VROC 7.5 Upgrade Key - Supported NVMe* RAID Features

NVMe* RAID Major Features	Standard Intel® VROC 7.5 Key (iPC – VROCSTANMOD)	Premium Intel® VROC 7.5 Key (iPC – VROCPREMMOD)	Intel® SSD Only VROC 7.5 Key (iPC – VROCISSDMOD)
Processor-attached NVMe* SSD – high performance	Yes	Yes	Yes
Boot on RAID volume	Yes	Yes	Yes
Third party vendor SSD support	Yes	Yes	No
RAID 0/1/10	Yes	Yes	Yes
RAID 0/1/5/10	No	Yes	Yes
RAID write hole closed (RMFBU replacement)	No	Yes	Yes
Hot plug/ surprise removal (2.5" SSD form factor only)	Yes	Yes	Yes
Enclosure LED management	Yes	Yes	Yes

9. System I/O

This chapter provides information on the server board's serial ports, USB ports, and Video support.

9.1 Serial Port Support

The server board supports two serial ports: Serial Port A and Serial Port B. Serial Port A is described below. For Serial Port B, see Section 6.3.

Serial Port A is an external RJ45 type connector on the back edge of the server board. The Serial Port A connector manufacturer is Foxconn* Interconnect Technology Limited; manufacturer part number is JMP1N07-RKM01-4H.

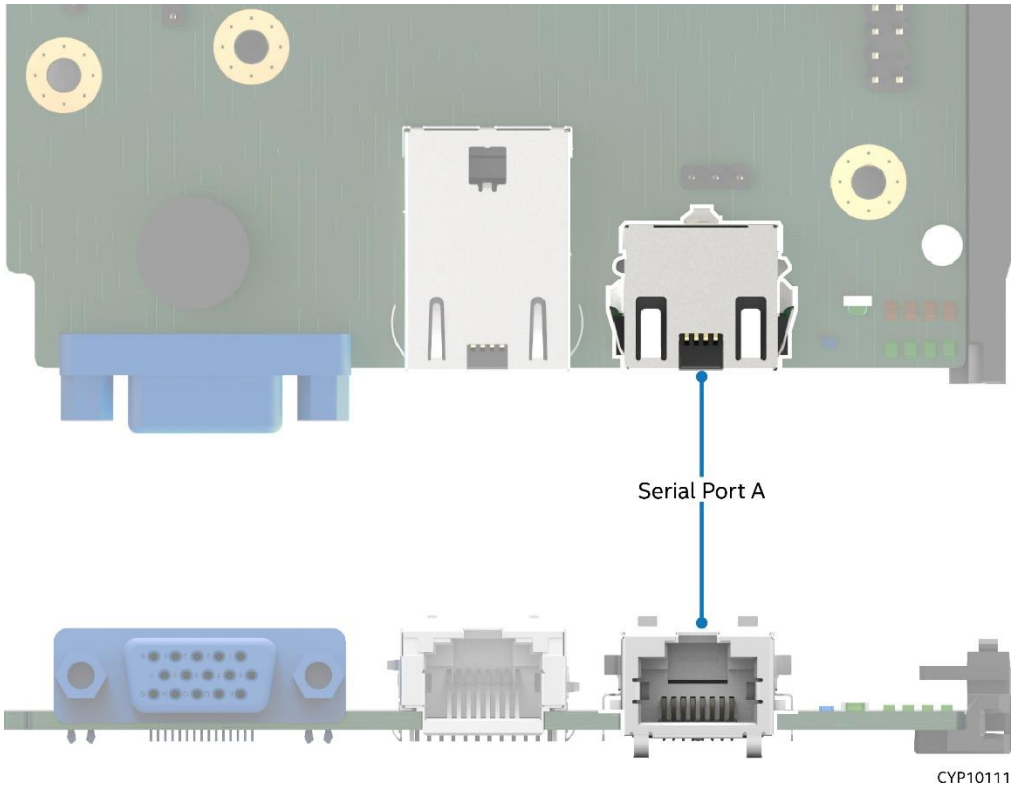


Figure 51. Serial port A

The pin orientation is shown in Figure 52 and the pinout is in Table 37.

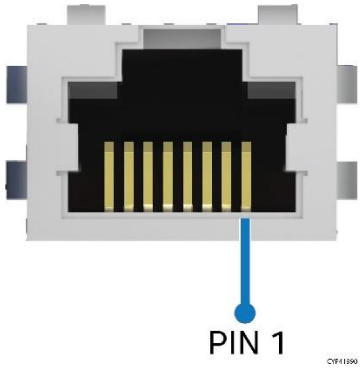


Figure 52. RJ45 Serial Port A Pin Orientation

Table 37. RJ45 Serial Port A Connector Pinout

Pin #	Signal Name	Pin #	Signal Name
1	RTS	**5**	RI
2	DTR	**6**	SIN
3	SOUT	**7**	DCD or DSR
4	GROUND	**8**	CTS

Note: Pin 7 of the RJ45 Serial Port-A connector is configurable to support either a DSR (default) signal or a DCD signal. The Pin 7 signal is changed by moving the jumper on the jumper header labeled "J4A2" from pins 1–2 (default) to pins 2–3 as shown in Figure 53.

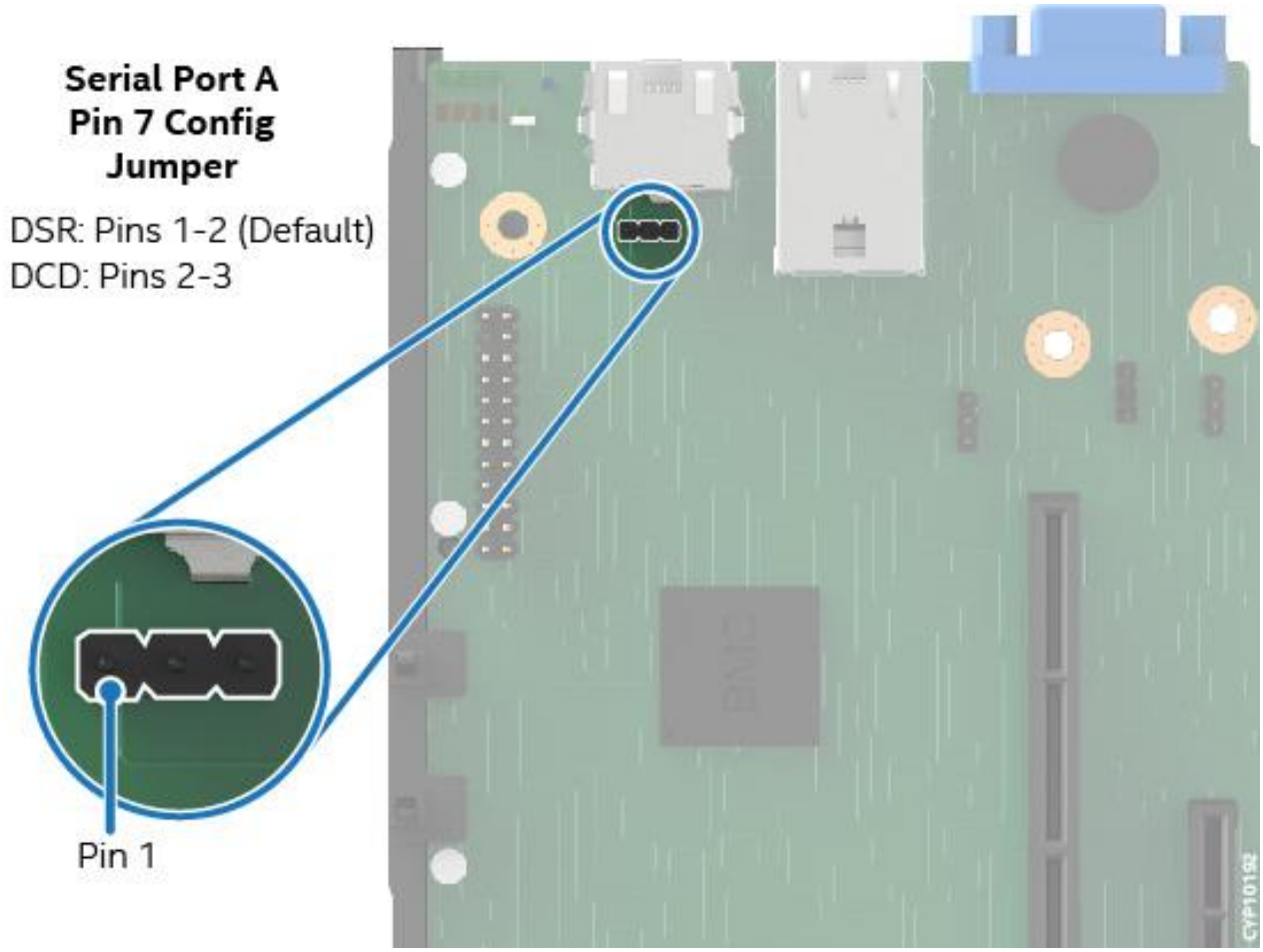


Figure 53. J4A2 Jumper Header for Serial Port A Pin 7 Configuration

9.2 USB Support

The following figure shows the three rear USB 3.0 ports on the server board. The following table provides the pinout for each connector. The connector manufacturer is Foxconn Interconnect Technology Limited; manufacturer part number is UEA11123-4HK3-4H.

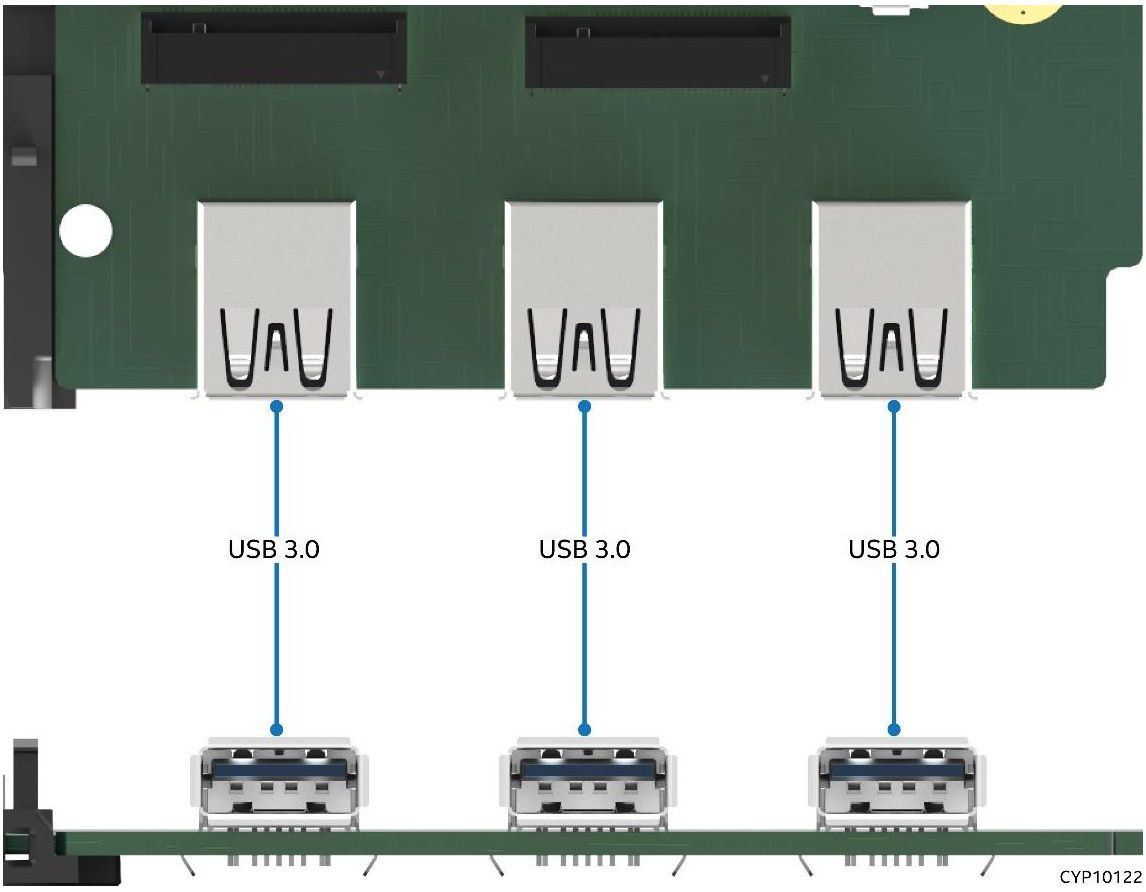


Figure 54. External USB 3.0 Connector Ports

Table 38. USB 3.0 Single Stack Rear Connector Pinout

Pin #	Signal Name
1	VBUS
2	D-
3	D+
4	GND
5	SSRX-

Pin #	Signal Name
6	SSRX+
7	GND_DRAIN
8	SSTX-
9	SSTX+

9.2.1 Internal USB 2.0 Type-A Connector

The server board includes one internal Type-A USB 2.0 connector. The following figure shows the connector location. The following table provides the pinout. The internal Type-A connector does not require 5 V Aux as it does not connect to a Human Interface Device (HID). The Serial Port A connector manufacturer is Foxconn Interconnect Technology Limited; manufacturer part number is UB01123-4BH1-4F.

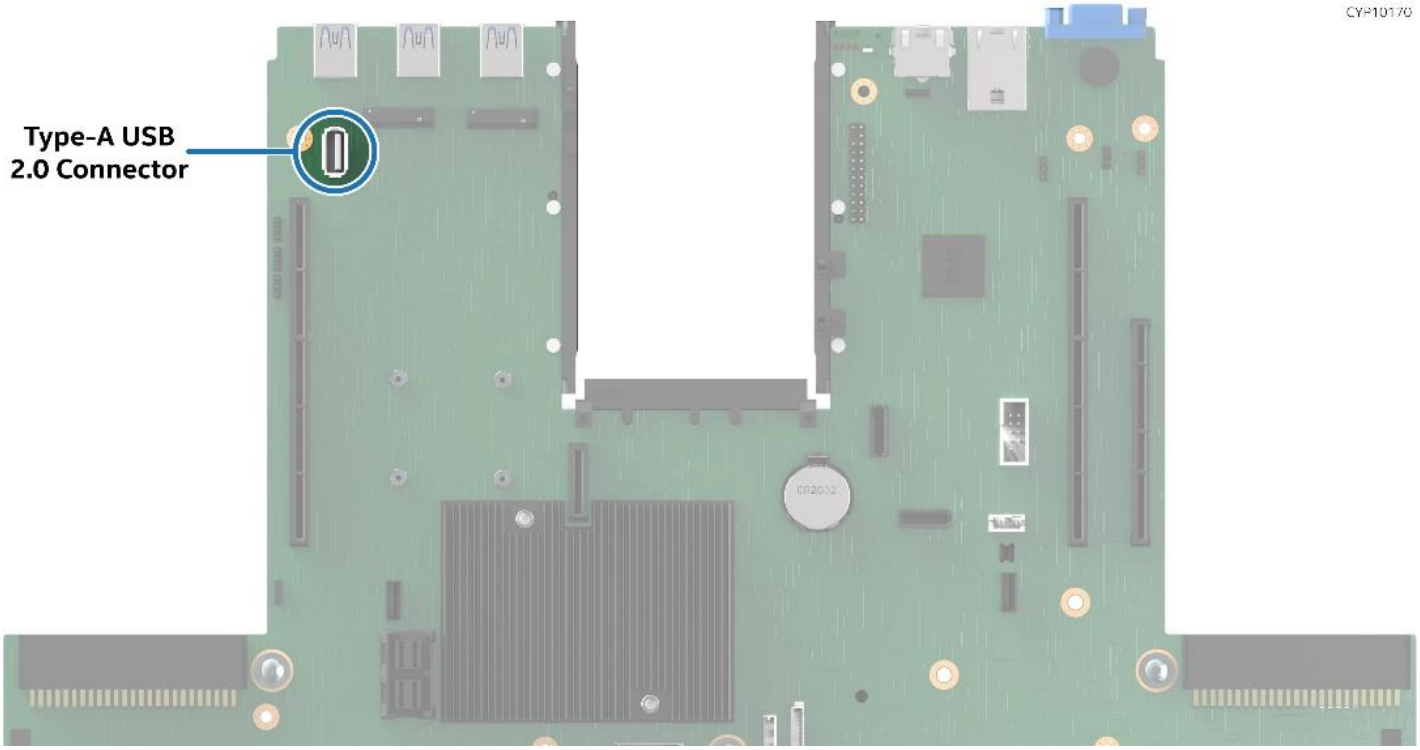


Figure 55. Internal USB 2.0 Type-A Connector

Table 39. Internal USB 2.0 Type-A Connector Pinout

Pin #	Signal Name
1	+5V
2	USB_N
3	USB_P
4	GND

9.3 Video Support

A standard 15-pin video connector is on the back edge of the server board.

9.3.1 Video Resolutions

The graphics controller of the ASPEED* AST2500 BMC is a VGA-compliant controller with 2D hardware acceleration and full bus master support. With 16 MB of memory reserved, the video controller supports the resolutions in the following table.

Table 40. Supported Video Resolutions

2D Mode Resolution	2D Video Support (Color Bit)			
	8 bpp	16 bpp	24 bpp	32 bpp
640 x 480	60, 72, 75, 85	60, 72, 75, 85	Not Supported	60, 72, 75, 85
800 x 600	60, 72, 75, 85	60, 72, 75, 85	Not Supported	60, 72, 75, 85
1024 x 768	60, 72, 75, 85	60, 72, 75, 85	Not Supported	60, 72, 75, 85
1152 x 864	75	75	75	75
1280 x 800	60	60	60	60
1280 x 1024	60	60	60	60
1440 x 900	60	60	60	60
1600 x 1200	60	60	Not Supported	Not Supported
1680 x 1050	60	60	Not Supported	Not Supported
1920 x 1080	60	60	Not Supported	Not Supported
1920 x 1200	60	60	Not Supported	Not Supported

9.3.2 Server Board Video and Add-In Video Adapter Support

The server board includes a standard 15-pin video connector on the back edge of the board.

BIOS Setup includes options to support the desired video operation when an add-in video card is installed.

- When both the **Onboard Video** and **Add-in Video Adapter** options are set to **Enabled**, both video displays can be active. The onboard video is still the primary console and active during BIOS POST. The add-in video adapter is only active under an operating system environment with video driver support.
- When **Onboard Video** is **Enabled** and **Add-in Video Adapter** is **Disabled**, only the onboard video is active.
- When **Onboard Video** is **Disabled** and **Add-in Video Adapter** is **Enabled**, only the add-in video adapter is active.

Configurations with add-in video cards can get more complicated with a dual processor socket board. Some multi-socket boards have PCIe* slots capable of hosting an add-in video card that is attached to the IIOs of processor sockets other than processor Socket 1. However, only one processor socket can be designated as a legacy VGA socket as required in POST. To provide for this situation, there is the PCI Configuration option **Legacy VGA Socket**. The rules for this option are:

- The **Legacy VGA Socket** option is grayed out and unavailable unless an add-in video card is installed in a PCIe* slot supported by CPU 1.
- Because the onboard video is hardwired to CPU 0, when **Legacy VGA Socket** is set to **CPU Socket 1**, the onboard video is disabled.

9.3.3 Dual Monitor Support

The BIOS supports single and dual video when add-in video adapters are installed. BIOS Setup does not have an enable/disable option for dual video. It works when both the **Onboard Video** and **Add-in Video Adapter** options are enabled.

In the single video mode, the onboard video controller or the add-in video adapter is detected during POST.

In dual video mode, the onboard video controller is enabled and is the primary video device. The add-in video adapter is allocated resources and is considered as the secondary video device during POST. The add-in video adapter is not active until the operating system environment is loaded.

9.4 Intel® Ethernet Network Adapter for OCP* Support

The server board supports several types of Intel® Ethernet Network Adapters. The adapters adhere to the OCP* specification and have a special connector that allows them to be installed to the OCP card slot on the server board. These cards are compatible with the Open Compute Project* (OCP*) 3.0 specification.

Note: The adapters listed in the following table are supported. No other adapters are supported.

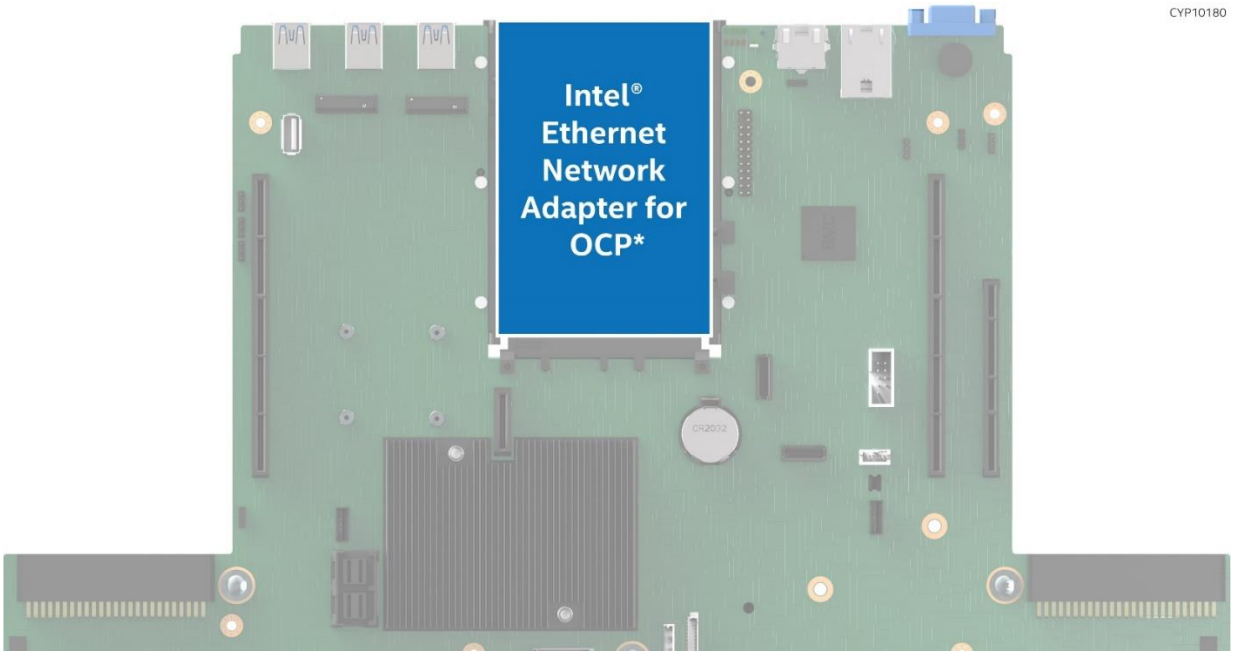


Figure 56. Intel® Ethernet Network Adapter for OCP* Placement

Table 41. Supported Intel® Ethernet Network Adapters for OCP*

Description	Interface	iPC
Dual port, RJ45, 10/1 GbE	PCIe* 3.0	X710T2LOCPV3
Quad port, SFP+ DA, 4x 10 GbE	PCIe* 3.0	X710DA4OCPV3
Dual Port, QSFP28 100/50/25/10 GbE	PCIe* 4.0	E810CQDA2OCPV3
Dual Port, SFP28 25/10 GbE	PCIe* 4.0	E810XXVDA2OCPV3

10. Intel® Light Guided Diagnostics

This chapter provides information on diagnostic LEDs on the server board. The following figure shows the location of the LEDs on the server boards: post code diagnostic LEDs, system ID LED, CPU 0 and CPU 1 fault LEDs, and fan fault LEDs (for 8-pin fan connectors).

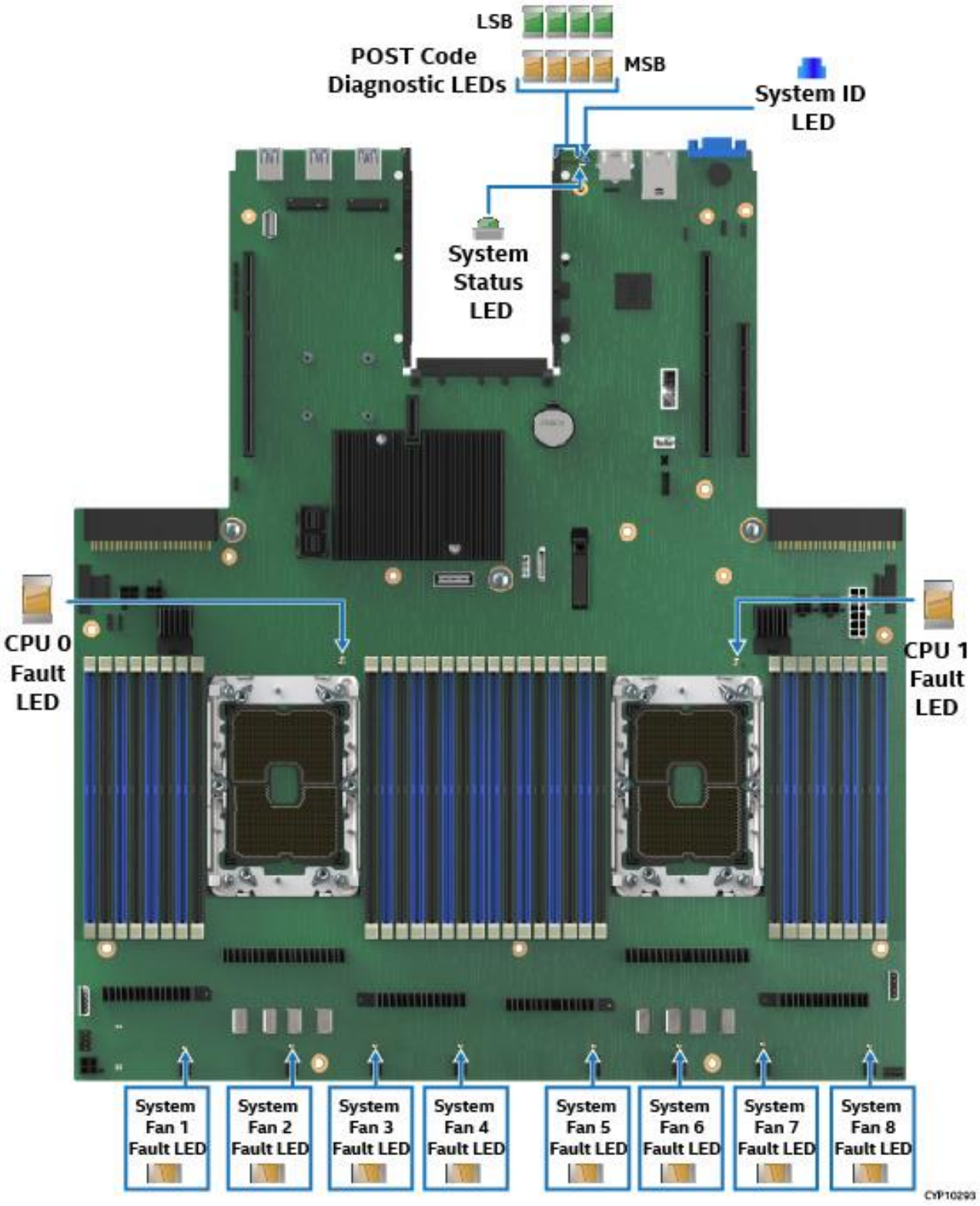


Figure 57. Intel® Light-Guided Diagnostics – LED Identification

The following figure provides an exploded view of the POST code Diagnostic, System ID, and System Status LEDs area.

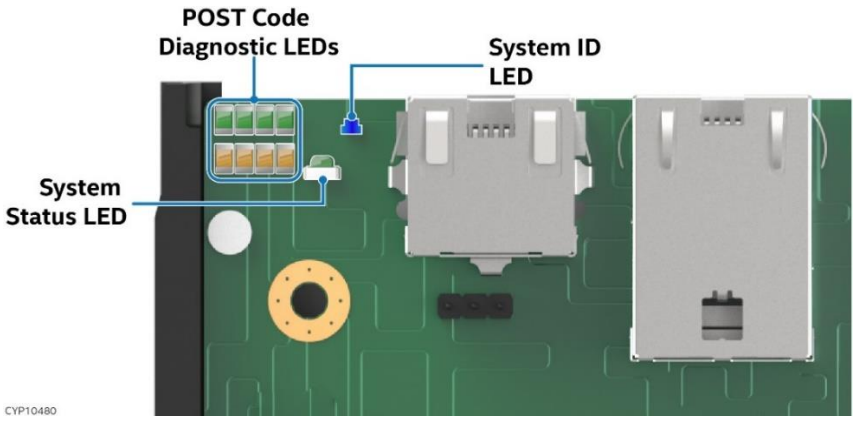


Figure 58. Exploded View of POST Code Diagnostic, System ID, and System Status LED Area

10.1 Post Code Diagnostic LEDs

A bank of eight POST code diagnostic LEDs are on the back edge of the server next to the Serial Port A connector. During the system boot process, the BIOS executes many platform configuration steps, each of which is assigned a specific hexadecimal POST code number. As each configuration step is started, the BIOS displays the given POST code to the POST code diagnostic LEDs. The purpose of these LEDs is to assist in troubleshooting a system hang condition during the POST process. The diagnostic LEDs can be used to identify the last POST process to be executed. See Appendix C for a complete description of how these LEDs are read, and for a list of all supported POST codes.

10.2 System ID LED

The server board includes a blue system ID LED that is used to visually identify a specific server system installed among many other similar systems.

Note: In an Intel Server System M50CYP2UR or M50CYP1UR family, there are two options available for illuminating the System ID LED:

- The front panel ID LED button is pushed that causes the LED to illuminate to a solid on state until the button is pushed again.
- An IPMI Chassis Identify command is remotely entered that causes the LED to blink.

10.3 System Status LED

The server board includes a bi-color system status LED. This LED indicates the current health of the server. Possible LED states include solid green, blinking green, solid amber, and blinking amber.

When the server is powered down (transitions to the DC-off state or S5), the BMC is still on standby power and retains the sensor and front panel status LED state established before the power-down event.

When source power is first applied to the system, the status LED turns solid amber and then immediately changes to blinking green to indicate that the BMC is booting. If the BMC boot process completes with no errors, the status LED changes to solid green.

Note: In an Intel Server System M50CYP2UR or M50CYP1UR family, the system status LED on the server board is tied directly to the system status LED on the front panel.

The following table lists and describes the states of the system status LED.

Table 42. System Status LED State Definitions

LED State	System State	BIOS Status Description
Off	No AC Power to system	• System power is not present. • System is in EuP Lot6 off mode. • System is in S5 soft-off state.
Solid green	System is operating normally.	• System is running (in S0 State) and its status is healthy. The system is not exhibiting any errors. Source power is present, BMC has booted, and manageability functionality is up and running. • After a BMC reset, and in conjunction with the chassis ID solid on, the BMC is booting Linux*. Control has been passed from BMC uBoot to BMC Linux*. It is in this state for roughly 10–20 seconds.
Blinking green	System is operating in a degraded state although still functioning, or system is operating in a redundant state but with an impending failure warning.	• Redundancy loss such as power-supply or fan. Applies only if the associated platform subsystem has redundancy capabilities. • Fan warning or failure when the number of fully operational fans is less than the minimum number needed to cool the system. • Non-critical threshold crossed – Temperature (including HSBP temp), voltage, input power to power supply, output current for main power rail from power supply and Processor Thermal Control (Therm Ctrl) sensors. • Power supply predictive failure occurred while redundant power supply configuration was present. • Unable to use all installed memory (more than 1 DIMM installed). • Correctable Errors over a threshold and migrating to a spare DIMM (memory sparing). This indicates that the system no longer has spared DIMMs (a redundancy lost condition). Corresponding DIMM LED lit. • In mirrored configuration, when memory mirroring takes place and system loses memory redundancy. • Battery failure. • BMC executing in uBoot. (Indicated by Chassis ID blinking at 3 Hz while Status blinking at 1 Hz). System in degraded state (no manageability). BMC uBoot is running but has not transferred control to BMC Linux*. Server will be in this state 6–8 seconds after BMC reset while it pulls the Linux* image into flash. • BMC Watchdog has reset the BMC. • Power Unit sensor offset for configuration error is asserted. • SSD Hot Swap Controller is off-line or degraded.
Blinking green and amber alternativel	System is initializing after source power is applied	• PFR in the process of updating/authenticating/recovering when source power is connected. system firmware being updated. • System not ready to take power button event/signal.
Blinking amber	System is operating in a degraded state with an impending failure warning, although still functioning. System is likely to fail.	• Critical threshold crossed – Voltage, temperature (including HSBP temp), input power to power supply, output current for main power rail from power supply and PROCHOT (Therm Ctrl) sensors. • VRD Hot asserted. • Minimum number of fans to cool the system not present or failed. • Hard drive fault. • Power Unit Redundancy sensor – Insufficient resources offset (indicates not enough power supplies present). • In non-sparing and non-mirroring mode, if the threshold of correctable errors is crossed within the window. • Invalid firmware image detected during boot up or firmware update

LED State	System State	BIOS Status Description

Solid amber	Critical/non-recoverable – system is halted. Fatal alarm – system has failed or shut down.	• Processor CATERR signal asserted.
		• MSID mismatch detected (CATERR also asserts for this case).
		• CPU 0 is missing.
		• Processor Thermal Trip.
		• No power good – power fault.
		• DIMM failure when there is only 1 DIMM present and hence no good memory present.
		• Runtime memory uncorrectable error in non-redundant mode.
		• DIMM Thermal Trip or equivalent.
		• SSB Thermal Trip or equivalent.
		• Processor ERR2 signal asserted.
		• BMC/Video memory test failed. (Chassis ID shows blue/solid-on for this condition.)
		• Both uBoot BMC firmware images are bad. (Chassis ID shows blue/solid-on for this condition.)
		• 240 VA fault.
		• Fatal Error in processor initialization:
		  ○ Processor family not identical
		  ○ Processor model not identical
		  ○ Processor core/thread counts not identical
		  ○ Processor cache size not identical
		  ○ Unable to synchronize processor frequency
		  ○ Unable to synchronize QPI link frequency
		• BMC fail authentication with non-recoverable condition, system hang at T-1; boot PCH only, system hang; PIT failed, system lockdown.

10.4 BMC Boot / Reset Status LED Indicators

During the BMC boot or BMC reset process, the system status LED and System ID LED are used to indicate BMC boot process transitions and states (if present). A BMC boot occurs when the AC power is first applied. (DC power on/off does not reset BMC.) BMC reset occurs after a BMC firmware update, on receiving a BMC cold reset command, and following a reset initiated by the BMC watchdog. The following table defines the LED states during the BMC boot/reset process.

Table 43. BMC Boot / Reset Status LED Indicators

BMC Boot/Reset State	System ID LED	System Status LED	Comment
BMC/video memory test failed	Solid blue	Solid amber	Non-recoverable condition. Contact an Intel representative for information on replacing this motherboard.
Both universal bootloader (u-Boot) images bad	6 Hz blinking blue	Solid amber	Non-recoverable condition. Contact an Intel representative for information on replacing this motherboard.
BMC in u-Boot	3 Hz blinking blue	1 Hz blinking green	Blinking green indicates degraded state (no manageability), blinking blue indicates u-Boot is running but has not transferred control to BMC Linux*. Server will be in this state 6–8 seconds after BMC reset while it pulls the Linux* image into flash.
BMC booting Linux*	Solid blue	Solid green	After an AC cycle/BMC reset, indicates that the control has been passed from u-Boot to BMC Linux* itself. It will be in this state for 10-20 seconds.
End of BMC boot/reset process. Normal system operation	Off	Solid green	Indicates BMC Linux* has booted and manageability functionality is up and running. Fault/status LEDs operate as usual.

10.5 Processor Fault LEDs

The server board includes a processor fault LED for each processor socket. The processor fault LED is lit if an MSID mismatch error is detected (that is, processor power rating is incompatible with the board).

Component	Managed by	Color	State	Description
Processor Fault LEDs	BMC	Off	Off	Ok (no errors)
		Solid Amber	On	MSID mismatch

10.6 Memory Fault LEDs

The server board includes memory fault LEDs for each DIMM slot (see following figure). When the BIOS detects a memory fault condition, it sends an IPMI OEM command (`Set Fault Indication`) to the BMC to turn on the associated memory slot fault LED. These LEDs are only active when the system is in the on state. The BMC does not activate or change the state of the LEDs unless instructed by the BIOS.

Component	Managed by	Color	State	Description
Memory Fault LED	BMC	Off	Off	Memory working correctly
		Solid Amber	On	Memory failure – detected by BIOS

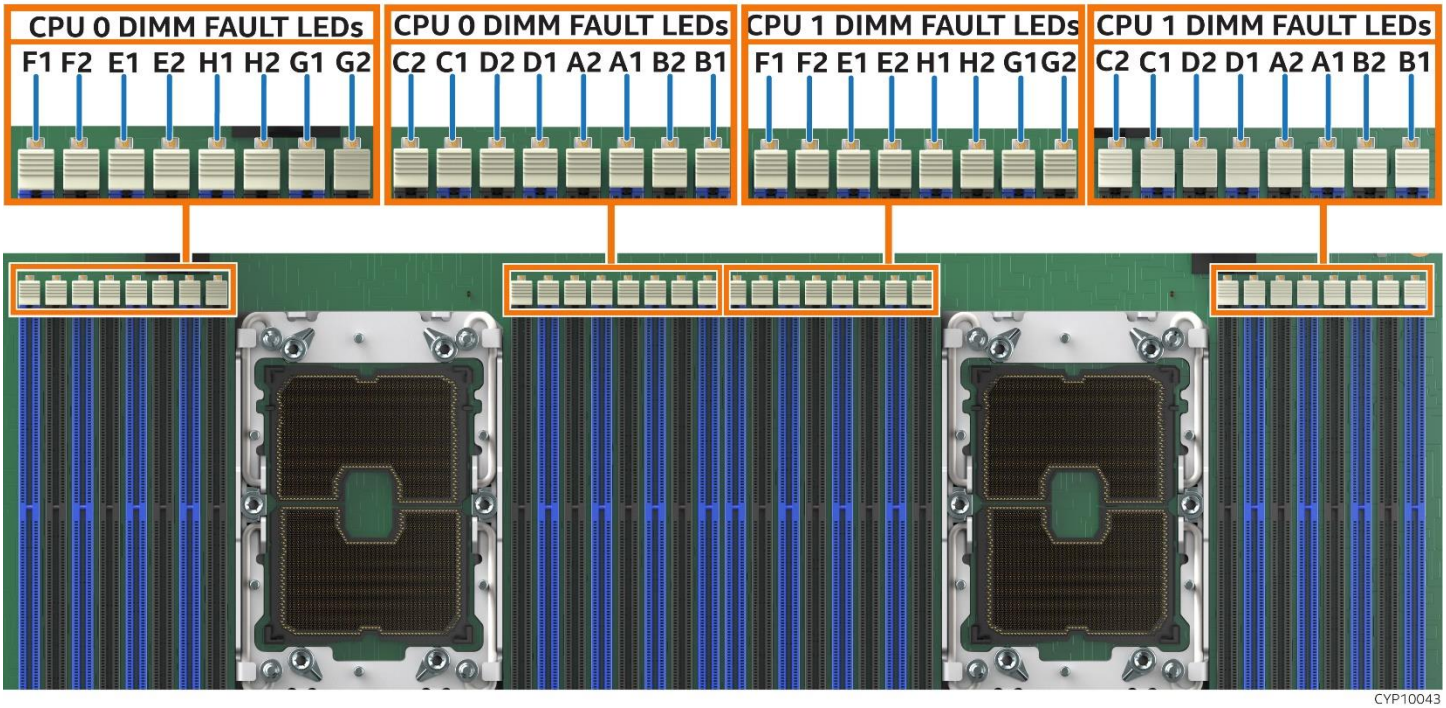


Figure 59. Memory Fault LED Location

10.7 Fan Fault LEDs

The following figure shows the fan fault LEDs associated with the 8-pin fan connectors. The BMC lights a fan fault LED if the associated fan-tach sensor has a lower critical threshold event status asserted. Fan-tach sensors are manual re-arm sensors. Once the lower critical threshold is crossed, the LED remains lit until the sensor is re-armed. These sensors are re-armed at system DC power-on and system reset.

Component	Managed by	Color	State	Description
Fan Fault LED	BMC	Off	Off	Fan working correctly
		Solid Amber	On	Fan failed

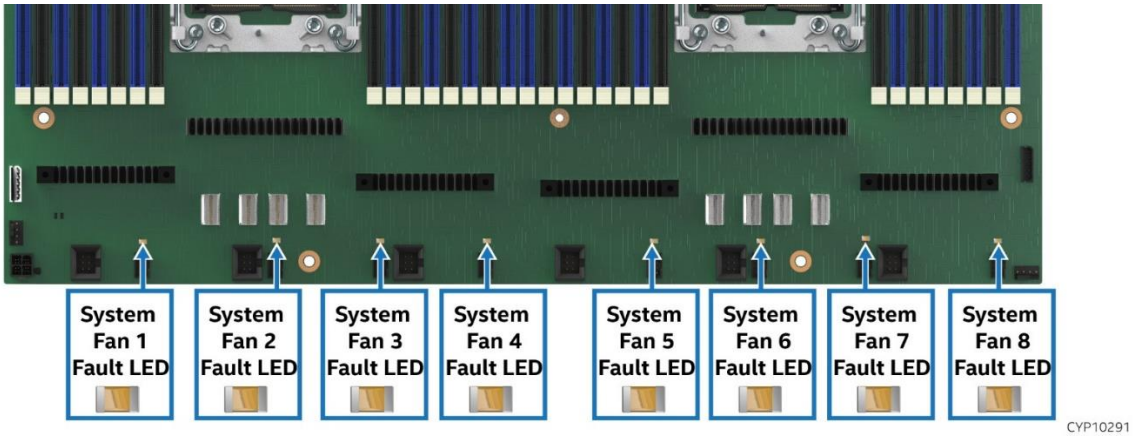


Figure 60. Fan Fault LEDs (Intel® Server Board M50CYP2SBSTD shown)

11. System Software Stack

The server board includes a system software stack that consists of the following components:

- System BIOS
- BMC firmware
- Intel® Management Engine (Intel® ME) firmware / Intel® Server Platform Services (Intel® SPS)
- Field replacement unit (FRU) and sensor data record (SDR) data.
- System CPLD firmware

Together, they configure and manage features and functions of the server system.

Many features and functions of the server system are managed jointly by the system BIOS and the BMC firmware, including:

- IPMI watchdog timer
- Messaging support, including command bridging and user/session support
- BIOS boot flags support
- Event receiver device: The BMC receives and processes events from the BIOS
- Serial-over-LAN (SOL)
- ACPI state synchronization: The BMC tracks ACPI state changes that are provided by the BIOS
- Fault resilient booting (FRB) – Fault resistant boot level 2 (FRB-2) is supported by the watchdog timer functionality
- DIMM temperature monitoring: New sensors and improved acoustic management using closed-loop fan control algorithm comprehending DIMM temperature readings
- Intel Intelligent Power Node Manager support
- Sensor and SEL logging additions/enhancements (such as, additional thermal monitoring capability)
- Embedded platform debug feature that allows capture of detailed data for later analysis by Intel

Note: Front panel management: In an Intel Server System M50CYP2UR or M50CYP1UR family, the BMC controls the system status LED and chassis ID LED. It supports secure lockout of certain front panel functionality and monitors button presses. The chassis ID LED is turned on using a front panel button or a command.

A factory installed software stack is pre-programmed on the server board during the board assembly process, making the server board functional at first power on. However, to ensure the most reliable system operation, it is highly recommended to check http://downloadcenter.intel.com for the latest available system updates and apply them before production deployment.

System updates can be performed in several operating environments, including the UEFI shell using the UEFI-only system update package (SUP), or under different operating systems using the System Firmware Update Package (SFUP) utility.

As part of the initial system integration process, system integrators must program system configuration data onto the server board using the FRUSDR utility. This action ensures the embedded platform management subsystem can provide the best performance and cooling for the final system configuration. The FRUSDR utility is included in the SUP and System Firmware Update Package (SFUP) packages. For additional information, see Section 11.2.

Refer to the following Intel documents for more in depth information about the system software stack and its functions:

- *BIOS Firmware External Product Specification (EPS) for the Intel® Server Board D50TNP and M50CYP Families* – Intel NDA required
- *Integrated Baseboard Management Controller Firmware External Product Specification (EPS) for the Intel® Server System D50TNP and M50CYP Families* – Intel NDA Required

11.1 Hot Keys Supported During POST

Certain hot keys are recognized during power-on self-test (POST). A hot key is a key or key combination that is recognized as an unprompted command input. In most cases, hot keys are recognized even while other processing is in progress.

BIOS supported hot keys are only recognized by the system BIOS during the system boot time POST process. Once the POST process has completed and transitions the system boot process to the operating system, BIOS supported hot keys are no longer recognized.

The following table provides a list of available POST hot keys along with a description for each.

Table 44. POST Hot Keys

Hot Key	Function
<F2>	Enter the BIOS Setup utility
<F6>	Pop-up BIOS boot menu
<F12>	Network boot
<Esc>	Switch from logo screen to diagnostic screen
<Pause>	Stop POST temporarily (press any key to resume)

11.1.1 POST Logo/Diagnostic Screen

If Quiet Boot is enabled in the BIOS Setup utility, a splash screen is displayed with the standard Intel logo screen or a customized original equipment manufacturer (OEM) logo screen, if one is present, in the designated flash memory location. By default, Quiet Boot is enabled in the BIOS Setup utility and the logo screen is the default POST display. However, pressing **<Esc>** hides the logo screen and displays the diagnostic screen instead during the current boot.

If a logo is not present in the BIOS flash memory space, or if Quiet Boot is disabled in the system configuration, the POST diagnostic screen is displayed with a summary of system configuration information. The POST diagnostic screen is purely a text mode screen, as opposed to the graphics mode logo screen.

If console redirection is enabled in the BIOS Setup utility, the Quiet Boot setting is disregarded, and the text mode diagnostic screen is displayed unconditionally. This action is due to the limitations of console redirection that transfers data in a mode that is not graphics-compatible.

11.1.2 BIOS Boot Pop-Up Menu

The BIOS boot selection (BBS) menu provides a boot device pop-up menu that is invoked by pressing the **<F6>** key during POST. The BBS pop-up menu displays all available boot devices. The boot order in the pop-up menu is not the same as the boot order in the BIOS Setup utility. The pop-up menu simply lists all the available devices from which the system can be booted and allows a manual selection of the desired boot device.

When an administrator password is configured in the BIOS Setup utility, the administrator password is required to access the boot pop-up menu. If a user password is entered, the user is taken directly to the boot manager in the BIOS Setup utility, only allowing booting in the order previously defined by the administrator.

11.1.3 Entering BIOS Setup

To enter the BIOS Setup utility using a keyboard (or emulated keyboard), press the **<F2>** function key during boot time when the OEM or Intel logo screen or the POST diagnostic screen is displayed.

The following instructional message is displayed on the diagnostic screen or under the Quiet Boot logo screen:

```
Press <F2> to enter setup, <F6> Boot Menu, <F12> Network Boot
```

Note: With a USB keyboard, it is important to wait until the BIOS discovers the keyboard and beeps. Until the USB controller has been initialized and the keyboard activated, key presses are not read by the system.

When the BIOS Setup utility is entered, the main screen is displayed initially. However, if a serious error occurs during POST, the system enters the BIOS Setup utility and displays the error manager screen instead of the main screen.

For additional BIOS Setup utility information, see the *BIOS Setup Utility User Guide for the Intel® Server Board D50TNP and M50CYP Families.*

11.1.4 BIOS Update Capability

To bring BIOS fixes or new features into the system, it is necessary to replace the current installed BIOS image with an updated one. Full BIOS update instructions are provided with update packages downloaded from the Intel website.

11.2 Field Replaceable Unit (FRU) and Sensor Data Record (SDR) Data

As part of the initial system integration process, the server board/system must have the proper FRU and SDR data loaded. This action ensures that the embedded platform management system can monitor the appropriate sensor data and operate the system with best cooling and performance. Once the system integrator has performed an initial FRU SDR package update, subsequent auto-configuration occurs without the need to perform additional SDR updates or provide other user input to the system when any of the following components are added or removed:

- Processor
- Memory
- OCP module
- Integrated SAS RAID module
- Power supply
- Fan
- Hot-swap backplane
- Front panel

Note: The system may not operate with best performance or best/appropriate cooling if the proper FRU and SDR data is not installed.

11.2.1 Loading FRU and SDR Data

The FRU and SDR data can be updated using a stand-alone FRUSDR utility in the UEFI shell or can be done using the System Firmware Update Package (SFUP) utility program under a supported operating system. Full FRU and SDR update instructions are provided with the appropriate system update package (SUP) or System Firmware Update Package (SFUP) that can be downloaded from http://downloadcenter.intel.com.

12. System Security

The server board supports a variety of system security options designed to prevent unauthorized system access or tampering of server settings. System security options supported include:

- Password protection
- Front panel lockout
- Intel® Platform Firmware Resilience (Intel® PFR)
- Intel® Software Guard Extensions (Intel® SGX)
- Intel® Total Memory Encryption (Intel® TME)
- Trusted Platform Module (TPM) support
- Intel® CBnT – Converged Intel® Boot Guard and Trusted Execution Technology (Intel® TXT)
- Unified Extensible Firmware Interface (UEFI) Secure Boot Technology

12.1 Password Protection

The BIOS Setup utility includes a Security tab where options to configure passwords, front panel lockout, and TPM settings, can be found.

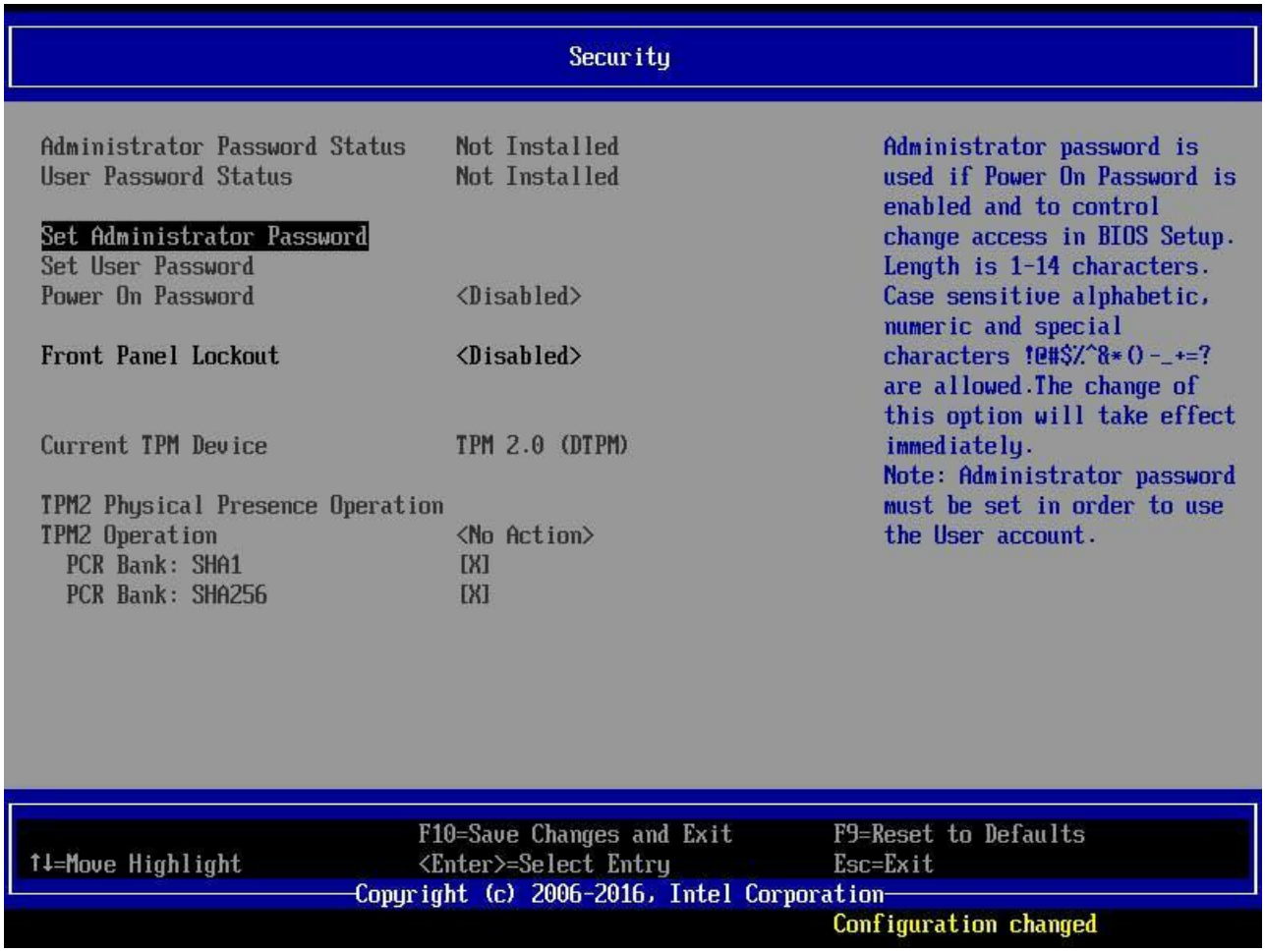


Figure 61. BIOS Setup Security Tab

12.1.1 Password Setup

The BIOS uses passwords to prevent unauthorized access to the server board. Passwords can restrict entry to the BIOS Setup utility, restrict use of the Boot Device popup menu during POST, suppress automatic USB device re-ordering, and prevent unauthorized system power-on. It is strongly recommended that an administrator password be set. A system with no administrator password set allows anyone who has access to the server board to change BIOS settings.

An administrator password must be set in order to set the user password.

The maximum length of a password is 14 characters. The minimum length is one character. The password can be made up of a combination of alphanumeric (a-z, A-Z, 0–9) characters and any of the following special characters:

! @ # $ % ^ & * ( ) - _ + = ?

Passwords are case sensitive.

The administrator and user passwords must be different from each other. An error message is displayed, and a different password must be entered if there is an attempt to enter the same password for both. The use of strong passwords is encouraged, but not required. To meet the criteria for a strong password, the password entered must be at least eight characters in length. It must include at least one each of alphabetic, numeric, and special characters. If a weak password is entered, a warning message is displayed, and the weak password is accepted. Once set, a password can be cleared by changing it to a null string. This action requires the administrator password and must be done through BIOS Setup. Clearing the administrator password also clears the user password. Passwords can also be cleared by using the password clear jumper on the server board. For more information on the password clear jumper, see Section 13.2.

Resetting the BIOS configuration settings to default values (by any method) has no effect on the administrator and user passwords.

As a security measure, if a user or administrator enters an incorrect password three times in a row during the boot sequence, the system is placed into a halt state. A system reset is required to exit out of the halt state. This feature makes it more difficult to guess or break a password.

In addition, on the next successful reboot, the Error Manager displays a Major Error code 0048. A SEL event is also logged to alert the authorized user or administrator that a password access failure has occurred.

12.1.2 System Administrator Password Rights

When the correct administrator password is entered, the user may perform the following actions:

- Access the BIOS Setup utility.
- Configure all BIOS Setup options in the BIOS Setup utility.
- Clear both the administrator and user passwords.
- Access the Boot Menu during POST.

If the Power On Password function is enabled in BIOS Setup, the BIOS halts early in POST to request a password (administrator or user) before continuing POST.

12.1.3 Authorized System User Password Rights and Restrictions

When the correct user password is entered, the user can perform the following actions:

- Access the BIOS Setup utility.
- View, but not change, any BIOS Setup options in the BIOS Setup utility.
- Modify system time and date in the BIOS Setup utility.

If the Power On Password function is enabled in BIOS Setup, the BIOS halts early in POST to request a password (administrator or user) before continuing POST.

Configuring an administrator password imposes restrictions on booting the system and configures most setup fields to read-only if the administrator password is not provided. The boot popup menu requires the administrator password to function, and the USB reordering is suppressed as long as the administrator password is enabled. Users are restricted from booting in anything other than the boot order defined in setup by an administrator.

12.2 Front Panel Lockout

If enabled in BIOS Setup from the Security screen, this option disables the following front panel features:

- The off function of the power button.
- System reset button.

If front panel lockout is enabled, system power off and reset must be controlled via a system management interface.

12.3 Intel® Platform Firmware Resilience (Intel® PFR)

As the intensity, sophistication, and disruptive impact of security attacks continue to escalate, data centers are driving a holistic approach to protect their critical infrastructure. This includes protecting server systems at the firmware level, the lowest layers of the platform, where threats are most difficult to detect. To address this situation, Intel has developed Intel® Platform Firmware Resilience (Intel® PFR) technology where platforms can provide security starting with power-on, system boot, and operating system load activities.

The Intel® Server Board M50CYP2SB family supports Intel® PFR technology, a hardware-enhanced platform security that uses an Intel® FPGA to protect, detect, and recover platform firmware.

- **Protect:** Monitors and filters malicious traffic on system buses. All platform firmware is attested safe before code execution.
- **Detect:** Verifies integrity of platform firmware images before executing. Performs boot and runtime monitoring to assure server is running a known good firmware.
- **Recover:** Automatically restores corrupted firmware from a protected gold recovery image within minutes.

Critical firmware elements protected in an Intel® Server Board M50CYP2SB family include: BIOS, SPI Descriptor, BMC, Intel® Management Engine (Intel® ME), and Power Supply firmware. This capability to mitigate firmware corruption is an important industry innovation and provides an optimal solution for security-sensitive organizations.

Intel® PFR fully supports the National Institute of Standards and Technology (NIST*) proposed firmware resiliency guidelines (SP 800-193) that have wide industry support.

12.4 Intel® Total Memory Encryption (Intel® TME)

To better protect computer system memory, the 3rd Gen Intel® Xeon® Scalable processor has a security feature called Intel® Total Memory Encryption (Intel® TME). This feature is supported on the Intel® Server Board M50CYP2SB family. Intel® TME helps ensure that all memory accessed from the Intel® processors is encrypted, including customer credentials, encryption keys, and other IP or personal information on the external memory bus. Intel® TME is also available for multi-tenant server platforms, called Intel® Total Memory Encryption – Multi-Tenant (Intel® TME-MT).

Intel developed this feature to provide greater protection for system memory against hardware attacks, such as removing and reading the dual in-line memory module (DIMM) after spraying it with liquid nitrogen or installing purpose-built attack hardware. Using the National Institute of Standards and Technology (NIST) storage encryption standard AES XTS, an encryption key is generated using a hardened random number generator in the processor without exposure to software. This allows existing software to run unmodified while better protecting memory.

Intel® TME can be enabled directly in the server BIOS and is compatible with Intel® Software Guard Extensions application enclave solutions.

Intel® TME has the following characteristics:

- **Encrypts** the entire memory using a NIST standard “storage-class” algorithm for encryption: AES-XTS
- **Transparent to software**, it encrypts data before writing to server memory and then decrypts on read.
- **Easy enablement** that requires no operating system or application enabling and is applicable to all operating systems.

To enable/disable Intel® TME, access the BIOS Setup menu by pressing **<F2>** key during POST. Navigate to the following menu: **Advanced > Processor Configuration**

Important Note: When either Intel® TME or Intel® TME-MT is enabled, a subset of memory RAS features and Intel® Optane™ persistent memory 200 series (if installed) will be disabled. See Table 13 for details.

For more information on Intel® TME, see the *BIOS Setup Utility User Guide for the Intel® Server Board D50TNP and M50CYP Families* and the *BIOS Firmware External Product Specification (EPS) for the Intel® Server Board D50TNP and M50CYP Families.*

12.5 Intel® Software Guard Extensions (Intel® SGX)

Intel® Software Guard Extensions (Intel® SGX) is a set of instructions that increases the security of application code and data, giving them more protection from disclosure or modification. Developers can partition sensitive information into enclaves that are areas of execution in memory with more security protection.

Intel® SGX Helps protect selected code and data from disclosure or modification. Intel® SGX helps partition applications into enclaves in memory that increase security. Enclaves have hardware-assisted confidentiality and integrity-added protections to help prevent access from processes at higher privilege levels. Through attestation services, a relying party can receive some verification on the identity of an application enclave before launch.

The Intel® Server Board M50CYP2SB family provides Intel® SGX. Intel® SGX provides fine grain data protection via application isolation in memory. Data protected includes code, transactions, IDs, keys, key material, private data, algorithms. Intel® SGX provides enhanced security protections for application data independent of operating system or hardware configuration. Intel® SGX provides the following security features:

- **Helps protect against attacks on software,** even if OS/drivers/BIOS/VMM/SMM are compromised.
- **Increases protections for secrets,** even when the attacker has full control of platform.
- **Helps prevent attacks**, such as memory bus snooping, memory tampering, and "cold boot" attacks, against memory contents in RAM.
- **Provides an option for hardware-based attestation** capabilities to measure and verify valid code and data signatures.

Intel® SGX for Intel® Xeon® Scalable processors are optimized to meet the application isolation needs of server systems in cloud environments:

- Massively increased electronic product code (enclave) size (up to 1 TB for typical 2-socket server system).
- Significant performance improvements: minimal impact vs native non-encrypted execution (significantly reduced overhead depending on workload).
- Fully software and binary-compatibility with applications written on other variants of Intel® SGX.
- Support for deployers to control which enclaves can be launched.
- Provides deployers full control over Attestation stack, compatible with Intel® Data Center Attestation primitives.
- Full protection against cyber (software) attacks, some reduction in protection against physical attacks (no integrity/anti-replay protections) vs other Intel SGX variants.
- Designed for environments where the physical environment is still trusted.

Note: Intel® SGX can only be enabled when Intel® TME is enabled. See Section 12.4 to enable Intel® TME

To enable/disable Intel® SGX, access the BIOS Setup menu by pressing the **<F2>** key during POST. Navigate to the following menu: **Advanced > Processor Configuration**

Important Note: When either Intel® TME or Intel® TME-MT is enabled, a subset of memory RAS features and Intel® Optane™ persistent memory 200 series (if installed) will be disabled. See Table 13 for details.

For more information on Intel® SGX, refer to the *BIOS Setup Utility User Guide for the Intel® Server Board D50TNP and M50CYP Families* and the *BIOS Firmware External Product Specification (EPS) for the Intel® Server Board D50TNP and M50CYP Families.*

12.6 Trusted Platform Module (TPM) Support

The Trusted Platform Module (TPM) option is a hardware-based security device that addresses the growing concern about boot process integrity and offers better data protection. TPM protects the system startup process by ensuring it is tamper-free before releasing system control to the operating system. A TPM device provides secured storage to store data, such as security keys and passwords. In addition, a TPM device has encryption and hash functions. The server board implements TPM as per *TPM PC Client Specifications revision 2.0,* published by the Trusted Computing Group (TCG).

A TPM device is optionally installed on the server board and is secured from external software attacks and physical theft. A pre-boot environment, such as the BIOS and operating system loader, uses the TPM to collect and store unique measurements from multiple factors within the boot process to create a system

fingerprint. This unique fingerprint remains the same unless the pre-boot environment is tampered with. Therefore, it is used to compare to future measurements to verify the integrity of the boot process.

After the system BIOS completes the measurement of its boot process, it hands off control to the operating system loader and, in turn, to the operating system. If the operating system is TPM-enabled, it compares the BIOS TPM measurements to those of previous boots to make sure the system was not tampered with before continuing the operating system boot process. Once the operating system is in operation, it optionally uses the TPM to provide additional system and data security (for example, Microsoft Windows* 10 supports BitLocker* drive encryption).

12.6.1 Trusted Platform Module (TPM) Security BIOS

The BIOS TPM support conforms to the TPM PC Client Implementation Specification for Conventional BIOS the TPM Interface Specification, and the Microsoft Windows* BitLocker* Requirements. The role of the BIOS for TPM security includes the following:

- Measures and stores the boot process in the TPM microcontroller to allow a TPM-enabled operating system to verify system boot integrity.
- Produces Extensible Firmware Interface (EFI) to a TPM-enabled operating system for using TPM.
- Produces Advanced Configuration and Power Interface (ACPI) TPM device and methods to allow a TPM-enabled operating system to send TPM administrative command requests to the BIOS.
- Verifies operator physical presence. Confirms and executes operating system TPM administrative command requests.
- Provides BIOS Setup options to change TPM security states and to clear TPM ownership.

For additional details, see the *TCG PC Client Specific Implementation Specification*, the *TCG PC Client Specific Physical Presence Interface Specification*, and the *Microsoft Windows* BitLocker* Requirements* documents.

12.6.2 Physical Presence

Administrative operations to the TPM require TPM ownership or physical presence indication by the operator to confirm the execution of administrative operations. The BIOS implements the operator presence indication by verifying the setup administrator password.

A TPM administrative sequence invoked from the operating system proceeds as follows:

1. A user makes a TPM administrative request through the operating system's security software.
2. The operating system requests the BIOS to execute the TPM administrative command through TPM ACPI methods and then resets the system.
3. The BIOS verifies the physical presence and confirms the command with the operator.
4. The BIOS executes TPM administrative command, inhibits BIOS Setup entry, and boots directly to the operating system that requested the TPM command.

12.6.3 TPM Security Setup Options

The BIOS TPM setup allows the operator to view the current TPM state and to carry out rudimentary TPM administrative operations. Performing TPM administrative options through the BIOS Setup requires TPM physical presence verification.

Using the BIOS TPM setup, the operator can turn TPM functionality On or Off and clear the TPM ownership contents. After the requested BIOS TPM setup operation is carried out, the option reverts to No Operation.

The BIOS TPM setup also displays the current state of the TPM, whether TPM is enabled or disabled and activated or deactivated. While using TPM, a TPM-enabled operating system or application may change the TPM state independently of the BIOS Setup. When an operating system modifies the TPM state, the BIOS Setup displays the updated TPM state.

The BIOS Setup **TPM Clear** option allows the operator to clear the TPM ownership key and allows the operator to take control of the system with TPM. You use this option to clear security settings for a newly initialized system or to clear a system for which the TPM ownership security key was lost.

12.7 Intel® CBnT – Converged Intel® Boot Guard and Trusted Execution Technology (Intel® TXT)

Previous generation Intel servers supported Intel® Boot Guard and Intel® Trusted Execution Technology (Intel® TXT).

Intel® Boot Guard

- Provides mechanism to authenticate the initial BIOS Code, before BIOS starts
- Hardware-based Static Root of Trust for Measurement (SRTM)
- Defends against attackers replacing/modifying the platform firmware

Intel® TXT

- Provides the ability to attest the authenticity of a platform configuration and OS environment; Establish trust
- Hardware-based Dynamic Root of Trust for Measurement (DRTM)
- Defends against software-based attacks aimed at stealing sensitive information

The two security features combined included some redundancies and inefficiencies between them. With this product generation, Intel rearchitected and fused together the two technologies into Intel® CBnT (Converged Intel® Boot Guard and Trusted Execution Technology). Combining the two technologies into one made them more efficient, eliminated redundancies between them, simplified their implementation, and provided stronger protections.

For more information, visit
https://www.intel.com/content/www/us/en/support/articles/000025873/technologies.html

12.8 Unified Extensible Firmware Interface (UEFI) Secure Boot Technology

UEFI secure boot technology defines how a platform's firmware can authenticate a digitally signed UEFI image, such as an operating system loader or a UEFI driver stored in an option ROM. This provides the capability to ensure that those UEFI images are only loaded in an owner authorized fashion and provides a common means to ensure platform security and integrity over systems running UEFI-based firmware. The Intel Server Board M50CYP2SB family BIOS is compliant with the UEFI Specification 2.3.1 Errata C for UEFI secure boot feature.

UEFI secure boot requires native UEFI boot mode and it disables legacy Option ROM dispatch. By default, secure boot on Intel server boards is disabled as the default boot mode is legacy mode.

To enable / disable UEFI Secure Boot in the BIOS Setup menu, select **Boot Maintenance Manager** > **Advanced Boot Options** > **Secure Boot Configuration**.

For more information on UEFI Secure Boot Technology, refer to the *BIOS Setup Utility User Guide for the Intel® Server Board D50TNP and M50CYP Families* and the *BIOS Firmware External Product Specification (EPS) for the Intel® Server Board D50TNP and M50CYP Families.*

13. Server Board Configuration and Service Jumpers

The server board includes several jumper blocks to configure, protect, or recover specific features of the server board. The following figure identifies the location of each jumper block on the server board. Pin 1 of each jumper can be identified by the arrowhead (▼) silkscreened on the server board next to the pin. The following sections describe how each jumper is used.

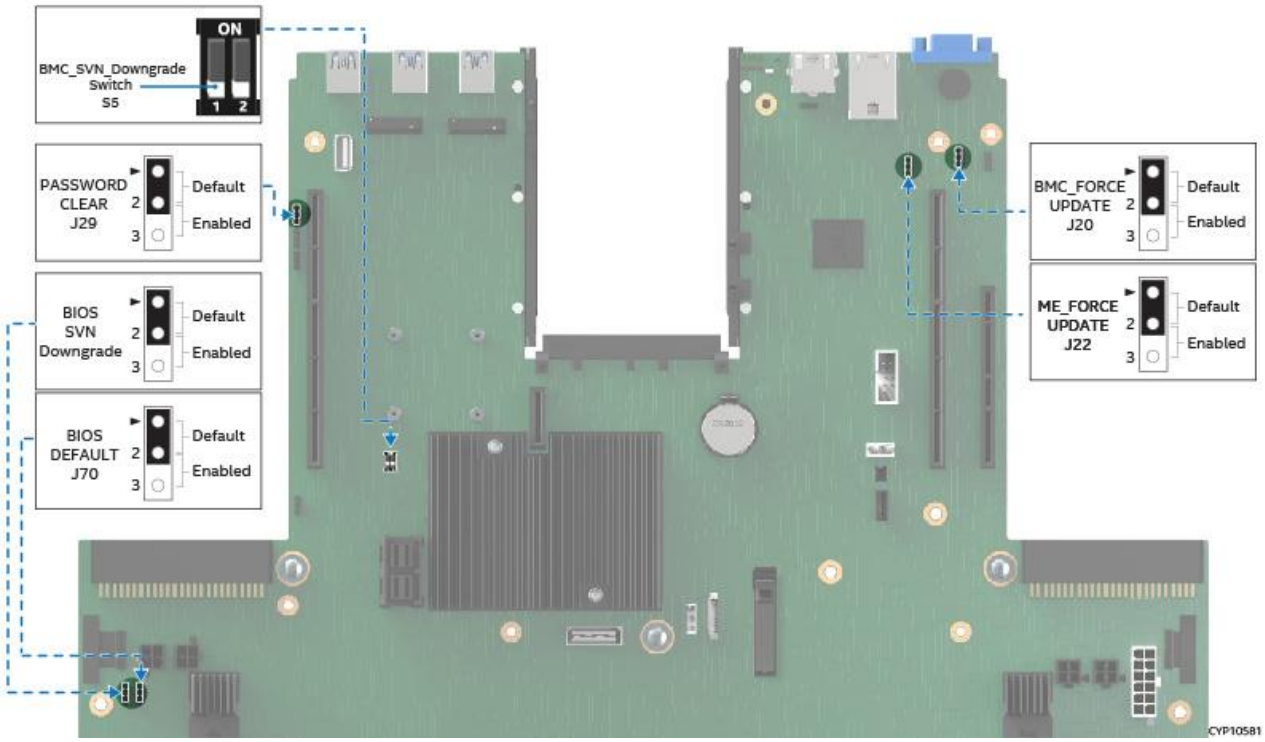


Figure 62. Reset and Recovery Jumper Header Locations

13.1 BIOS Default Jumper (BIOS DFLT – J70)

This jumper resets BIOS options, configured using the <F2> BIOS Setup Utility, back to their original default factory settings.

Note: This jumper does not reset administrator or user passwords. To reset passwords, the password clear jumper must be used.

To use the BIOS default jumper, perform the following steps:

1. Power down the server system
2. Unplug the power cord(s).
3. Remove the system top cover
4. Move the “BIOS DFLT” (J70) jumper from pins 1–2 (normal operation) to pins 2–3 (set BIOS defaults).
5. Wait five seconds, then move the jumper back to pins 1–2.
6. Reinstall the system top cover.
7. Reinstall system power cords.

   Note: The system automatically powers on after AC power is applied to the system.

8. Power on the system and press **<F2>** during POST to access the BIOS Setup utility to configure and save desired BIOS options.

After resetting BIOS options using the BIOS default jumper, the Error Manager Screen in the BIOS Setup utility displays two errors:

- 0012 System RTC date/time not set
- 5220 BIOS Settings reset to default settings

The system time and date will need to be reset.

13.2 Password Clear Jumper (PASSWD_CLR – J29)

This jumper causes both the user password and the administrator password to be cleared if they were set. The operator should be aware that this situation creates a security gap until passwords have been configured again through the BIOS Setup utility. This is the only method by which the administrator and user passwords can be cleared unconditionally. Other than this jumper, passwords can only be set or cleared by changing them explicitly in BIOS Setup. No method of resetting BIOS configuration settings to default values affects either the administrator or user passwords.

To use the password clear jumper, perform the following steps:

1. Power down the server system.
2. For safety, unplug the power cord(s).
3. Remove the system top cover.
4. Move the “PASSWD_CLR” (J29) jumper from pins 1–2 (default) to pins 2–3 (password clear position).
5. Reinstall the system top cover
6. Reattach the power cord(s).
7. Power up the server and press **<F2>** to access the BIOS Setup utility.
8. Verify the password clear operation was successful by viewing the Error Manager screen. Two errors should be logged:
   - 5221 Passwords cleared by jumper
   - 5224 Password clear jumper is set
9. Exit the BIOS Setup utility and power down the server.
10. For safety, remove the power cord(s)
11. Remove the system top cover.
12. Move the “PASSWD_CLR” (J29) jumper back to pins 1–2 (default).
13. Reinstall the system top cover
14. Reattach the power cord(s).
15. Power up the server system.
16. Intel strongly recommends to boot into BIOS Setup immediately, navigate to the Security tab, and set the administrator and user passwords if intending to use BIOS password protection.

13.3 Intel® Management Engine (Intel® ME) Firmware Force Update Jumper (ME_FRC_UPDT – J22)

When the Intel® ME firmware force update jumper is moved from its default position, the Intel® ME is forced to operate in a reduced minimal operating capacity. This jumper should only be used if the Intel® ME firmware has gotten corrupted and requires reinstallation.

Note: The Intel® ME image file is included in the system update packages (SUP) posted to Intel’s download center website at http://downloadcenter.intel.com.

To use the Intel® ME firmware force update jumper, perform the following steps:

1. Turn off the system
2. Remove the power cord(s).

Note: If the Intel® ME force update jumper is moved with power connected to the system, the Intel® ME will not operate properly.

3. Remove the system top cover.
4. Move the "ME FRC UPD" (J22) jumper from pins 1–2 (default) to pins 2–3 (force update position).
5. Reinstall the system top cover
6. Reattach the power cord(s).
7. Power on the system.
8. Boot to the EFI shell.
9. Change directories to the folder containing the update files.
10. Update the Intel® ME firmware using the following command:

    Sysfwupdt –u <version#>_UpdateCapsule.bin

11. When the update has successfully completed, power off the system.
12. Remove the power cord(s).
13. Remove the system top cover.
14. Move the "ME FRC UPD" (J22) jumper back to pins 1–2 (default).
15. Reinstall the system top cover
16. Reattach the power cord(s)
17. Power on the system.

13.4 BMC Force Update Jumper (BMC FRC UPD - J20)

The BMC force update jumper is used to put the BMC in boot recovery mode for a low-level update. It causes the BMC to abort its normal boot process and stay in the boot loader without executing any Linux* code. This jumper should only be used if the BMC firmware has become corrupted and requires reinstallation.

Note: The BMC image file is included in the SUP posted to Intel's download center website at http://downloadcenter.intel.com.

To use the BMC force update jumper, perform the following steps:

1. Turn off the system
2. Remove the power cord(s).

Note: If the BMC FRC UPD jumper is moved with power connected to the system, the BMC will not operate properly.

3. Remove the system top cover.
4. Move the "BMC FRC UPD" (J20) jumper from pins 1–2 (default) to pins 2–3 (force update position).
5. Reinstall the system top cover
6. Reattach the power cord(s).
7. Power on the system.
8. Boot to the EFI shell.
9. Change directories to the folder containing the update files.
10. Update the BMC firmware using the following command:

    sysfwupdt.efi -u <filename.bin>

11. When the update has successfully completed, power off the system.
12. Remove the power cord(s).
13. Remove the system top cover.
14. Move the “BMC FRC UPD” (J20) jumper back to pins 1–2 (default).
15. Reattach the power cord(s)
16. Power on the system.
17. Boot to the EFI shell.
18. Change directories to the folder containing the update files.
19. Reinstall the board/system SDR data by running the FRUSDR utility.
20. After the SDRs have been loaded, reboot the server.

13.5 BIOS SVN Downgrade Jumper (BIOS_SVN_DG – J71)

The BIOS SVN Downgrade Jumper is labeled SNV_BYPASS on the server board. When this jumper is moved from its default pin position (pins 1–2), it allows the server system firmware (including BIOS) in the PFR-controlled PCH capsule file to be downgraded to previous revisions. This jumper is used when there is a need for the server system to power on using previous revision BIOS.

Caution: Downgrading to an older version of BIOS may result in the loss of functionality and security features that are present in a later version but was not implemented in the older version.

Caution: When downgrading to an older version of BIOS, server systems may end up with a firmware stack combination that is not supported, and therefore could experience unpredictable behavior.

Note: Latest system update packages are included in the SUP posted to Intel’s download center website at http://downloadcenter.intel.com

---

To use the Security Version Number (SVN) Bypass jumper, perform the following steps:

1. Turn off the system.
2. Remove the chassis top cover panels.
3. Remove the air duct, if needed.
4. Remove the riser assemblies from the system, if needed.
   Refer to the *Intel® Server System M50CYP2UR Family Installation and Service Guide* for instructions.
5. Using a tweezers, move the “BIOS_SVN_DG” (J71) jumper from pins 1–2 (default) to pins 2–3 (SVN Bypass).
6. Reinstall the riser assemblies, if needed.
7. Power on the system. The system automatically boots to the EFI shell.
8. Update the BIOS using the standard BIOS update instructions provided with the system update package.
9. After the BIOS update has successfully completed, power down the system.
10. Remove the riser assemblies from the module.
11. Using a tweezers, move the “BIOS_SVN_DG” (J71) jumper back to pins 1–2 (default).
12. Reinstall the riser assemblies, if needed.
13. Reinstall the air duct, if needed.
14. Reinstall the chassis top cover panels.
15. Power on the system. During POST, press **<F2>** to access the BIOS Setup utility to configure and save desired BIOS options.

13.6 BMC SVN Downgrade Switch (BMC_SVN_DG – S5)

When BMC SVN Downgrade Switch (switch 1) is moved from its default Off position to the On position, it allows the system BMC firmware in the PFR-controlled BMC capsule file to be downgraded to a lower Security Version Number (SVN). This switch is used when there is a need for the system to power on using BMC revision with lower SVN.

Caution: Downgrading to a BMC version with lower SVN may result in the loss of functionality and security features that are present in a higher SVN but were not implemented in the lower SVN.

Caution: When downgrading to an older version of BMC, modules may end up with a firmware stack combination that is not supported, and therefore could experience unpredictable behavior.

Caution: Switch 2 is for debug purposes and must not be changed from its default Off position.

Note: Latest system update packages are included in the SUP posted to Intel's download center website at http://downloadcenter.intel.com

---

To use the BMC_SVN_DG Downgrade switch, perform the following steps:

1. Remove the chassis top cover.
2. Remove the air duct, if needed.
3. Remove the riser assemblies from the system, if needed.
4. Using a tweezers, move "BMC_SVN_DG" (S5) switch 1 to the On position.
5. Reinstall the riser assemblies, if needed.
6. Reinstall the air duct, if needed.
7. Reinstall the chassis top cover.
8. Power on the system. The system automatically boots to the EFI shell.
9. Update the BIOS using the standard BIOS update instructions provided with the system update package.
10. After the BIOS update has successfully completed, power down the system.
11. Remove the riser assemblies from the module.
12. Remove the chassis top cover.
13. Remove the air duct, if needed.
14. Using a tweezers, move "BMC_SVN_DG" (S5) switch 1 back to the Off position.
15. Reinstall the riser assemblies, if needed.
16. Reinstall the air duct, if needed.
17. Reinstall the chassis top cover.
18. Power on the system. During POST, press **<F2>** to access the BIOS Setup utility to configure and save desired BIOS options.

Appendix A. Getting Help

Available Intel support options with your Intel Server System:

1. 24x7 support through Intel's support webpage at https://www.intel.com/content/www/us/en/support/products/1201/server-products.html

   Information available at the support site includes:

   - Latest BIOS, firmware, drivers, and utilities
   - Product documentation, setup, and service guides
   - Full product specifications, technical advisories, and errata
   - Compatibility documentation for memory, hardware add-in cards, and operating systems
   - Server and chassis accessory parts list for ordering upgrades or spare parts
   - A searchable knowledge base to search for product information throughout the support site

   Quick Links:

Use the following links for support on Intel Server Boards and Server Systems	**Download Center** http://www.intel.com/support/downloadserversw	**BIOS Support Page** http://www.intel.com/support/serverbios	**Troubleshooting Boot Issue** http://www.intel.com/support/tsboot
Use the following links for support on Intel® Data Center Block (DCB) Integrated Systems* * Intel DCB comes pre-populated with processors, memory, storage, and peripherals based on how it was ordered through the Intel Configure to Order tool.	**Download Center** http://www.intel.com/support/downloaddcbsw	**Technical Support Documents** http://www.intel.com/support/dcb	**Warranty and Support Info** http://www.intel.com/support/dcbwarranty

2. If a solution cannot be found at Intel's support site, submit a service request via Intel's online service center at https://supporttickets.intel.com/servicecenter?lang=en-US. In addition, you can also view previous support requests. (Login required to access previous support requests)

3. Contact an Intel support representative using one of the support phone numbers available at https://www.intel.com/content/www/us/en/support/contact-support.html (charges may apply).

Intel also offers Partner Alliance Program members around-the-clock 24x7 technical phone support on Intel® server boards, server chassis, server RAID controller cards, and Intel® Server Management at https://www.intel.com/content/www/us/en/partner-alliance/overview.html

Note: The 24x7 support number is available after logging in to the Intel Partner Alliance website.

Warranty Information

To obtain warranty information, visit http://www.intel.com/p/en_US/support/warranty.

Appendix B. Integration and Usage Tips

This appendix provides a list of useful information that is unique to the Intel® Server Board M50CYP2SB family and should be kept in mind while configuring your server system.

- When adding or removing components or peripherals from the server board, power cords must be disconnected from the server. With power applied to the server, standby voltages are still present even though the server board is powered off.
- The server boards support the 3rd Gen Intel® Xeon® Scalable processor family with a Thermal Design Power (TDP) of up to and including 270 Watts. Previous generations of the Intel® Xeon® processor and Intel® Xeon® Scalable processor families are not supported. Server systems using these server boards may or may not meet the TDP design limits of the server board. Validate the TDP limits of the server system before selecting a processor.
- Processors must be installed in order. CPU 0 must be populated for the server board to operate.
- Riser Card Slots #2 and #3 on the server board can only be used in dual processor configurations.
- The riser card slots are specifically designed to support riser cards only. Attempting to install a PCIe* add-in card directly into a riser card slot on the server board may damage the server board, the add-in card, or both.
- For the best performance, the number of DDR4 DIMMs installed should be balanced across both processor sockets and memory channels.
- On the back edge of the server board, there are eight diagnostic LEDs that display a sequence of POST codes during the boot process. If the server board hangs during POST, the LEDs display the last POST event run before the hang.
- The system status LED is set to a steady amber color for all fatal errors that are detected during processor initialization. A steady amber system status LED indicates that an unrecoverable system failure condition has occurred.
- RAID partitions created using either Intel® VMD cannot span across the two embedded SATA controllers. Only drives attached to a common SATA controller can be included in a RAID partition.
- The FRUSDR utility must be run as part of the initial platform integration process before it is deployed into a live operating environment. Once the initial FRU and SDR data is loaded on to the system, all subsequent system configuration changes automatically update SDR data using the BMC auto configuration feature, without having to run the FRUSDR utility again. However, to ensure the latest sensor data is installed, the SDR data should be updated to the latest available as part of a planned system software update.
- Make sure the latest system software is loaded on the server. This includes system BIOS, BMC firmware, Intel® ME firmware and FRUSDR. The latest system software can be downloaded from http://downloadcenter.intel.com.

Appendix C. Post Code Diagnostic LED Decoder

As an aid in troubleshooting a system hang that occurs during a system POST process, the server board includes a bank of eight POST code diagnostic LEDs on the back edge of the server board.

During the system boot process, Memory Reference Code (MRC) and system BIOS execute several memory initialization and platform configuration routines, each of which is assigned a hex POST code number.

As each process is started, the given POST code number is displayed to the POST code diagnostic LEDs on the back edge of the server board.

During a POST system hang, the displayed POST code can be used to identify the last POST routine that was run before the error occurring, helping to isolate the possible cause of the hang condition.

Each POST code is represented by eight LEDs, four green LEDs and four amber LEDs. The POST codes are divided into two nibbles, an upper nibble and a lower nibble. The upper nibble bits are represented by amber diagnostic LEDs and the lower nibble bits are represented by green diagnostics LEDs. If the bit is set, the corresponding LED is lit. If the bit is clear, the corresponding LED is off. For each set of nibble bits, LED 0 represents the least significant bit (LSB) and LED 3 represents the most significant bit (MSB).

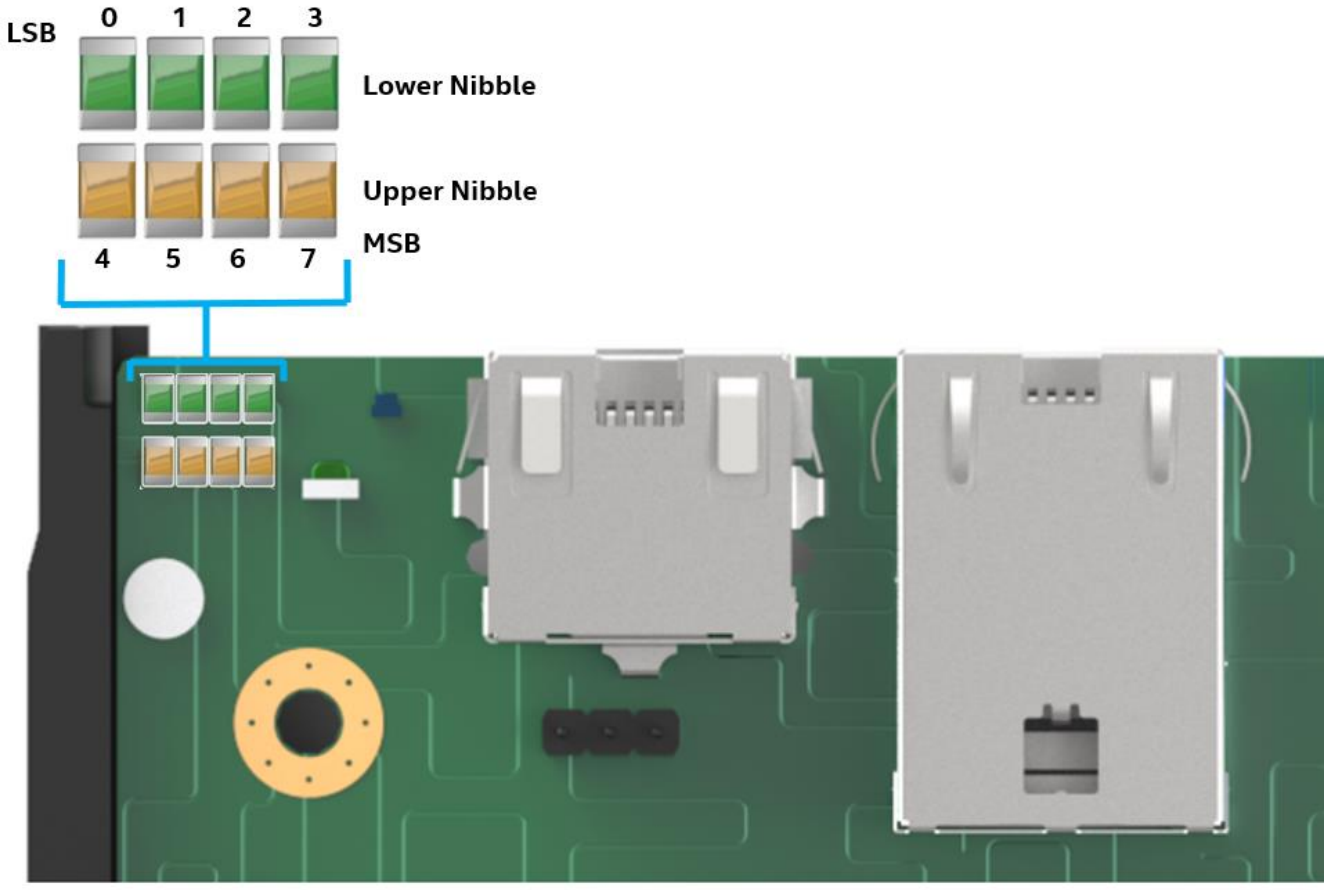


Figure 63. Server Board POST Diagnostic LEDs

Note: Diagnostic LEDs are best read and decoded when viewing the LEDs from the back of the system.

In the following example, the BIOS sends a value of AC to the diagnostic LED decoder. The LEDs are decoded as shown in the following table.

Table 45. POST Progress Code LED Example

LEDs		Upper Nibble AMBER LEDs				Lower Nibble GREEN LEDs			
		MSB							**LSB**
		LED #7	LED #6	LED #5	LED #4	LED #3	LED #2	LED #1	LED #0
		8h	4h	2h	1h	8h	4h	2h	1h
Status		**ON**	OFF	**ON**	OFF	**ON**	**ON**	OFF	OFF
Read Value	Binary	1	0	1	0	1	1	0	0
	Hexadecimal	**A**h				**C**h			
Result		**AC**h							

Upper nibble bits = 1010b = **A**h; Lower nibble bits = 1100b = **C**h; the two Hex Nibble values are combined to create a single **AC**h POST Progress Code.

C.1 Early POST Memory Initialization MRC Diagnostic Codes

Memory initialization at the beginning of POST includes multiple functions: discovery, channel training, validation that the DIMM population is acceptable and functional, initialization of the IMC and other hardware settings, and initialization of applicable RAS configurations.

The MRC progress codes are displayed to the diagnostic LEDs that show the execution point in the MRC operational path at each step.

Table 46. MRC Progress Codes

Post Code (Hex)	Upper Nibble				Lower Nibble				Description
	8h	4h	2h	1h	8h	4h	2h	1h	
B0	1	0	1	1	0	0	0	0	Detect DIMM population
B1	1	0	1	1	0	0	0	1	Set DDR4 frequency
B2	1	0	1	1	0	0	1	0	Gather remaining SPD data
B3	1	0	1	1	0	0	1	1	Program registers on the memory controller level
B4	1	0	1	1	0	1	0	0	Evaluate RAS modes and save rank information
B5	1	0	1	1	0	1	0	1	Program registers on the channel level
B6	1	0	1	1	0	1	1	0	Perform the JEDEC defined initialization sequence
B7	1	0	1	1	0	1	1	1	Train DDR4 ranks
1	0	0	0	0	0	0	0	1	Train DDR4 ranks
2	0	0	0	0	0	0	1	0	Train DDR4 ranks – Read DQ/DQS training
3	0	0	0	0	0	0	1	1	Train DDR4 ranks – Receive enable training
4	0	0	0	0	0	1	0	0	Train DDR4 ranks – Write DQ/DQS training
5	0	0	0	0	0	1	0	1	Train DDR4 ranks – DDR channel training done
B8	1	0	1	1	1	0	0	0	Initialize CLTT/OLTT
B9	1	0	1	1	1	0	0	1	Hardware memory test and init
BA	1	0	1	1	1	0	1	0	Execute software memory init
BB	1	0	1	1	1	0	1	1	Program memory map and interleaving
BC	1	0	1	1	1	1	0	0	Program RAS configuration
BE	1	0	1	1	1	1	1	0	Execute BSSA RMT
BF	1	0	1	1	1	1	1	1	MRC is done

If a major memory initialization error occurs, preventing the system from booting with data integrity, a beep code is generated, the MRC displays a fatal error code on the diagnostic LEDs, and a system halt command is executed. Fatal MRC error halts do not change the state of the system status LED and they do not get logged as SEL events. Table 47 lists all MRC fatal errors that are displayed to the diagnostic LEDs.

Note: Fatal MRC errors display POST error codes that may be the same as BIOS POST progress codes displayed later in the POST process. The fatal MRC codes can be distinguished from the BIOS POST progress codes by the accompanying memory failure beep code of three long beeps as identified in Table 47.

Table 47. MRC Fatal Error Codes

Post Code (Hex)	Upper Nibble				Lower Nibble				Description
	8h	4h	2h	1h	8h	4h	2h	1h	
E8	1	1	1	0	1	0	0	0	No usable memory error 01h = No memory was detected from SPD read, or invalid config that causes no operable memory. 02h = Memory DIMMs on all channels of all sockets are disabled due to hardware memtest error. 03h = No memory installed. All channels are disabled.
E9	1	1	1	0	1	0	0	1	Memory is locked by Intel® TXT and is inaccessible
EA	1	1	1	0	1	0	1	0	DDR4 channel training error 01h = Error on read DQ/DQS (Data/Data Strobe) init 02h = Error on Receive Enable 03h = Error on Write Leveling 04h = Error on write DQ/DQS (Data/Data Strobe
EB	1	1	1	0	1	0	1	1	Memory test failure 01h = Software memtest failure. 02h = Hardware memtest failed.
ED	1	1	1	0	1	1	0	1	DIMM configuration population error 01h = Different DIMM types (RDIMM, LRDIMM) are detected installed in the system. 02h = Violation of DIMM population rules. 03h = The 3rd DIMM slot cannot be populated when QR DIMMs are installed. 04h = UDIMMs are not supported. 05h = Unsupported DIMM Voltage.
EF	1	1	1	0	1	1	1	1	Indicates a CLTT table structure error

C.2 BIOS POST Progress Codes

The following table provides a list of all POST progress codes.

Table 48. POST Progress Codes

Post Code (Hex)	Upper Nibble				Lower Nibble				Description
	8h	4h	2h	1h	8h	4h	2h	1h	
SEC Phase									
01	0	0	0	0	0	0	0	1	First POST code after CPU reset
02	0	0	0	0	0	0	1	0	Microcode load begin
03	0	0	0	0	0	0	1	1	CRAM initialization begin
04	0	0	0	0	0	1	0	0	PEI Cache When Disabled
05	0	0	0	0	0	1	0	1	SEC Core At Power On Begin.
06	0	0	0	0	0	1	1	0	Early CPU initialization during SEC Phase.
UPI RC (Fully leverage without platform change)									
A1	1	0	1	0	0	0	0	1	Collect info such as SBSP, boot mode, reset type, etc.
A3	1	0	1	0	0	0	1	1	Setup minimum path between SBSP and other sockets
A6	1	0	1	0	0	1	1	0	Sync up with PBSPs
A7	1	0	1	0	0	1	1	1	Topology discovery and route calculation
A8	1	0	1	0	1	0	0	0	Program final route
A9	1	0	1	0	1	0	0	1	Program final IO SAD setting
AA	1	0	1	0	1	0	1	0	Protocol layer and other uncore settings
AB	1	0	1	0	1	0	1	1	Transition links to full speed operation
AE	1	0	1	0	1	1	1	0	Coherency settings
AF	1	0	1	0	1	1	1	1	KTI initialization done
PEI Phase									
10	0	0	0	1	0	0	0	0	PEI Core
11	0	0	0	1	0	0	0	1	CPU PEIM
15	0	0	0	1	0	1	0	1	Platform Type Init
19	0	0	0	1	1	0	0	1	Platform PEIM Init
Integrated I/O Progress Codes									
E0	1	1	1	0	0	0	0	0	Integrated I/O Early Init Entry
E1	1	1	1	0	0	0	0	1	Integrated I/O Pre-link Training
E2	1	1	1	0	0		1	0	Integrated I/O EQ Programming
E3	1	1	1	0	0	0	1	1	Integrated I/O Link Training
E4	1	1	1	0	0	1	0	0	Internal Use
E5	1	1	1	0	0	1	0	1	Integrated I/O Early Init Exit
E6	1	1	1	0	0	1	1	0	Integrated I/O Late Init Entry
E7	1	1	1	0	0	1	1	1	Integrated I/O PCIe Ports Init
E8	1	1	1	0	1	0	0	0	Integrated I/O IOAPIC init
E9	1	1	1	0	1	0	0	1	Integrated I/O VTD Init
EA	1	1	1	0	1	0	1	0	Integrated I/O IOAT Init
EB	1	1	1	0	1	0	1	1	Integrated I/O DXF Init
EC	1	1	1	0	1	1	0	0	Integrated I/O NTB Init
ED	1	1	1	0	1	1	0	1	Integrated I/O Security Init
EE	1	1	1	0	1	1	1	0	Integrated I/O Late Init Exit
EF	1	1	1	0	1	1	1	1	Integrated I/O ready to boot

Post Code (Hex)	Upper Nibble				Lower Nibble				Description
	8h	4h	2h	1h	8h	4h	2h	1h	
MRC Progress Codes – At this point the MRC Progress Code sequence is executed.									
31	0	0	1	1	0	0	0	1	Memory Installed
32	0	0	1	1	0	0	1	0	CPU PEIM (CPU Init)
33	0	0	1	1	0	0	1	1	CPU PEIM (Cache Init)
34	0	0	1	1	0	1	0	0	CPU BSP Select
35	0	0	1	1	0	1	0	1	CPU AP Init
36	0	0	1	1	0	1	1	0	CPU SMM Init
4F	0	1	0	0	1	1	1	1	DXE IPL started
Memory Feature Progress Codes									
C1	1	1	0	0	0	0	0	1	Memory POR check
C2	1	1	0	0	0	0	1	0	Internal Use
C3	1	1	0	0	0	0	1	1	Internal Use
C4	1	1	0	0	0	1	0	0	Internal Use
C5	1	1	0	0	0	1	0	1	Memory Early Init
C6	1	1	0	0	0	1	1	0	Display DIMM info in debug mode
C7	1	1	0	0	0	1	1	1	JEDEC Nvdimm training
C9	1	1	0	0	1	0	0	1	Setup SVL and Scrambling
CA	1	1	0	0	1	0	1	0	Internal Use
CB	1	1	0	0	1	0	1	1	Check RAS support
CC	1	1	0	0	1	1	0	0	Pmem ADR Init
CD	1	1	0	0	1	1	0	1	Internal Use
CE	1	1	0	0	1	1	1	0	Memory Late Init
CF	1	1	0	0	1	1	1	1	Determine MRC boot mode
D0	1	1	0	1	0	0	0	0	MKTME Early Init
D1	1	1	0	1	0	0	0	1	SGX Early Init
D2	1	1	0	1	0	0	1	0	Memory Margin Test
D3	1	1	0	1	0	0	1	1	Internal Use
D5	1	1	0	1	0	1	0	1	Internal Use
D6	1	1	0	1	0	1	1	0	Offset Training Result
DXE Phase									
60	0	1	1	0	0	0	0	0	DXE Core started
62	0	1	1	0	0	0	1	0	DXE Setup Init
68	0	1	1	0	1	0	0	0	DXE PCI Host Bridge Init
69	0	1	1	0	1	0	0	1	DXE NB Init
6A	0	1	1	0	1	0	1	0	DXE NB SMM Init
70	0	1	1	1	0	0	0	0	DXE SB Init
71	0	1	1	1	0	0	0	1	DXE SB SMM Init
72	0	1	1	1	0	0	1	0	DXE SB devices Init
78	0	1	1	1	1	0	0	0	DXE ACPI Init
79	0	1	1	1	1	0	0	1	DXE CSM Init
7D	0	1	1	1	1	1	0	1	DXE Removable Media Detect
7E	0	1	1	1	1	1	1	0	DXE Removable Media Detected
90	1	0	0	1	0	0	0	0	DXE BDS started
91	1	0	0	1	0	0	0	1	DXE BDS connect drivers
92	1	0	0	1	0	0	1	0	DXE PCI bus begin

Post Code (Hex)	Upper Nibble				Lower Nibble				Description
	8h	4h	2h	1h	8h	4h	2h	1h	
93	1	0	0	1	0	0	1	1	DXE PCI Bus HPC Init
94	1	0	0	1	0	1	0	0	DXE PCI Bus enumeration
95	1	0	0	1	0	1	0	1	DXE PCI Bus resource requested
96	1	0	0	1	0	1	1	0	DXE PCI Bus assign resource
97	1	0	0	1	0	1	1	1	DXE CON_OUT connect
98	1	0	0	1	1	0	0	0	DXE CON_IN connect
99	1	0	0	1	1	0	0	1	DXE SIO Init
9A	1	0	0	1	1	0	1	0	DXE USB start
9B	1	0	0	1	1	0	1	1	DXE USB reset
9C	1	0	0	1	1	1	0	0	DXE USB detect
9D	1	0	0	1	1	1	0	1	DXE USB enable
A1	1	0	1	0	0	0	0	1	DXE IDE begin
A2	1	0	1	0	0	0	1	0	DXE IDE reset
A3	1	0	1	0	0	0	1	1	DXE IDE detect
A4	1	0	1	0	0	1	0	0	DXE IDE enable
A5	1	0	1	0	0	1	0	1	DXE SCSI begin
A6	1	0	1	0	0	1	1	0	DXE SCSI reset
A7	1	0	1	0	0	1	1	1	DXE SCSI detect
A8	1	0	1	0	1	0	0	0	DXE SCSI enable
AB	1	0	1	0	1	0	1	1	DXE SETUP start
AC	1	0	1	0	1	1	0	0	DXE SETUP input wait
AD	1	0	1	0	1	1	0	1	DXE Ready to Boot
AE	1	0	1	0	1	1	1	0	DXE Legacy Boot
AF	1	0	1	0	1	1	1	1	DXE Exit Boot Services
B0	1	0	1	1	0	0	0	0	RT Set Virtual Address Map Begin
B1	1	0	1	1	0	0	0	1	RT Set Virtual Address Map End
B2	1	0	1	1	0	0	1	0	DXE Legacy Option ROM init
B3	1	0	1	1	0	0	1	1	DXE Reset system
B4	1	0	1	1	0	1	0	0	DXE USB Hot plug
B5	1	0	1	1	0	1	0	1	DXE PCI BUS Hot plug
B8	1	0	1	1	1	0	0	0	PWRBTN Shutdown
B9	1	0	1	1	1	0	0	1	SLEEP Shutdown
C0	1	1	0	0	0	0	0	0	End of DXE
C7	1	1	0	0	0	1	1	1	DXE ACPI Enable
0	0	0	0	0	0	0	0	0	Clear POST Code
S3 Resume									
E0	1	1	1	0	0	0	0	0	S3 Resume PEIM (S3 started)
E1	1	1	1	0	0	0	0	1	S3 Resume PEIM (S3 boot script)
E2	1	1	1	0	0	0	1	0	S3 Resume PEIM (S3 Video Repost)
E3	1	1	1	0	0	0	1	1	S3 Resume PEIM (S3 OS wake)

Appendix D. Post Code Errors

Most error conditions encountered during POST are reported using POST error codes. These codes represent specific failures, warnings, or information. POST error codes may be displayed in the error manager display screen and are always logged to the System Event Log (SEL). Logged events are available to system management applications, including remote and Out of Band (OOB) management.

There are exception cases in early initialization where system resources are not adequately initialized for handling POST Error Code reporting. These cases are primarily fatal error conditions resulting from initialization of processors and memory, and they are handed by a diagnostic LED display with a system halt.

Table 49 lists the supported POST error codes. Each error code is assigned an error type that determines the action the BIOS takes when the error is encountered. Error types include minor, major, and fatal. The BIOS action for each is defined as follows:

- **Minor**: An error message may be displayed to the screen or to the BIOS Setup Error Manager and the POST error code is logged to the SEL. The system continues booting in a degraded state. The user may want to replace the erroneous unit. The "POST Error Pause" option setting in the BIOS Setup does not have any effect on this error.
- **Major**: An error message is displayed to the Error Manager screen and an error is logged to the SEL. If the BIOS Setup option "Post Error Pause" is enabled, operator intervention is required to continue booting the system. If the BIOS Setup option "POST Error Pause" is disabled, the system continues to boot.

  Note: For 0048 "Password check failed", the system halts and then, after the next reset/reboot, displays the error code on the Error Manager screen.

- **Fatal**: If the system cannot boot, POST halts and displays the following message:
  `Unrecoverable fatal error found. System will not boot until the error is resolved.`
  Press **<F2>** to enter setup.

  When the **<F2>** key on the keyboard is pressed, the error message is displayed on the Error Manager screen and an error is logged to the system event log (SEL) with the POST error code. The system cannot boot unless the error is resolved. The faulty component must be replaced. The "POST Error Pause" option setting in the BIOS Setup does not have any effect on this error.

Note: The POST error codes in the following table are common to all current generation Intel® server platforms. Features present on a given server board/system determine which of the listed error codes are supported.

Table 49. POST Error Messages and Handling

Error Code	Error Message	Action message	Type
0012	System RTC date/time not set		Major
0048	Password check failed	Put right password.	Major
0140	PCI component encountered a PERR error		Major
0141	PCI resource conflict		Major
0146	PCI out of resources error	Enable Memory Mapped I/O above 4 GB item at SETUP to use 64-bit MMIO.	Major
0191	Processor core/thread count mismatch detected	Use identical CPU type.	Fatal
0192	Processor cache size mismatch detected	Use identical CPU type.	Fatal
0194	Processor family mismatch detected	Use identical CPU type.	Fatal
0195	Processor Intel(R) UPI link frequencies unable to synchronize		Fatal
0196	Processor model mismatch detected	Use identical CPU type.	Fatal
0197	Processor frequencies unable to synchronize	Use identical CPU type.	Fatal
5220	BIOS Settings reset to default settings		Major
5221	Passwords cleared by jumper		Major
5224	Password clear jumper is Set	Recommend reminding user to install BIOS password as BIOS admin password is the master keys for several BIOS security features.	Major
8130	CPU 0 disabled		Major
8131	CPU 1 disabled		Major
8160	CPU 0 unable to apply microcode update		Major
8161	CPU 1 unable to apply microcode update		Major
8170	CPU 0 failed Self-Test (BIST)		Major
8171	CPU 1 failed Self-Test (BIST)		Major
8180	CPU 0 microcode update not found		Minor
8181	CPU 1 microcode update not found		Minor
8190	Watchdog timer failed on last boot.		Major
8198	OS boot watchdog timer failure.		Major
8300	Baseboard Management Controller failed self-test.		Major
8305	Hot Swap Controller failure		Major
83A0	Management Engine (ME) failed self-test.		Major
83A1	Management Engine (ME) Failed to respond.		Major
84F2	Baseboard management controller failed to respond		Major
84F3	Baseboard Management Controller in Update Mode.		Major
84F4	Baseboard Management Controller Sensor Data Record empty.	Update right SDR.	Major
84FF	System Event Log full	Clear SEL through EWS or SELVIEW utility.	Minor
85FC	Memory component could not be configured in the selected RAS mode		Major
8501	Memory Population Error	Plug DIMM at right population.	Major
8502	PMem invalid DIMM population found on the system.	Populate valid POR PMem DIMM population.	Major
8520	Memory failed test/initialization CPU0_DIMM_A1	Remove the disabled DIMM.	Major
8521	Memory failed test/initialization CPU0_DIMM_A2	Remove the disabled DIMM.	Major
8522	Memory failed test/initialization CPU0_DIMM_A3	Remove the disabled DIMM.	Major

Error Code	Error Message	Action message	Type
8523	Memory failed test/initialization CPU0_DIMM_B1	Remove the disabled DIMM.	Major
8524	Memory failed test/initialization CPU0_DIMM_B2	Remove the disabled DIMM.	Major
8525	Memory failed test/initialization CPU0_DIMM_B3	Remove the disabled DIMM.	Major
8526	Memory failed test/initialization CPU0_DIMM_C1	Remove the disabled DIMM.	Major
8527	Memory failed test/initialization CPU0_DIMM_C2	Remove the disabled DIMM.	Major
8528	Memory failed test/initialization CPU0_DIMM_C3	Remove the disabled DIMM.	Major
8529	Memory failed test/initialization CPU0_DIMM_D1	Remove the disabled DIMM.	Major
852A	Memory failed test/initialization CPU0_DIMM_D2	Remove the disabled DIMM.	Major
852B	Memory failed test/initialization CPU0_DIMM_D3	Remove the disabled DIMM.	Major
852C	Memory failed test/initialization CPU0_DIMM_E1	Remove the disabled DIMM.	Major
852D	Memory failed test/initialization CPU0_DIMM_E2	Remove the disabled DIMM.	Major
852E	Memory failed test/initialization CPU0_DIMM_E3	Remove the disabled DIMM.	Major
852F	Memory failed test/initialization CPU0_DIMM_F1	Remove the disabled DIMM.	Major
8530	Memory failed test/initialization CPU0_DIMM_F2	Remove the disabled DIMM.	Major
8531	Memory failed test/initialization CPU0_DIMM_F3	Remove the disabled DIMM.	Major
8532	Memory failed test/initialization CPU0_DIMM_G1	Remove the disabled DIMM.	Major
8533	Memory failed test/initialization CPU0_DIMM_G2	Remove the disabled DIMM.	Major
8534	Memory failed test/initialization CPU0_DIMM_G3	Remove the disabled DIMM.	Major
8535	Memory failed test/initialization CPU0_DIMM_H1	Remove the disabled DIMM.	Major
8536	Memory failed test/initialization CPU0_DIMM_H2	Remove the disabled DIMM.	Major
8537	Memory failed test/initialization CPU0_DIMM_H3	Remove the disabled DIMM.	Major
8538	Memory failed test/initialization CPU1_DIMM_A1	Remove the disabled DIMM.	Major
8539	Memory failed test/initialization CPU1_DIMM_A2	Remove the disabled DIMM.	Major
853A	Memory failed test/initialization CPU1_DIMM_A3	Remove the disabled DIMM.	Major
853B	Memory failed test/initialization CPU1_DIMM_B1	Remove the disabled DIMM.	Major
853C	Memory failed test/initialization CPU1_DIMM_B2	Remove the disabled DIMM.	Major
853D	Memory failed test/initialization CPU1_DIMM_B3	Remove the disabled DIMM.	Major
853E	Memory failed test/initialization CPU1_DIMM_C1	Remove the disabled DIMM.	Major
853F (Go to 85C0)	Memory failed test/initialization CPU1_DIMM_C2	Remove the disabled DIMM.	Major
8540	Memory disabled.CPU0_DIMM_A1	Remove the disabled DIMM.	Major
8541	Memory disabled.CPU0_DIMM_A2	Remove the disabled DIMM.	Major
8542	Memory disabled.CPU0_DIMM_A3	Remove the disabled DIMM.	Major
8543	Memory disabled.CPU0_DIMM_B1	Remove the disabled DIMM.	Major
8544	Memory disabled.CPU0_DIMM_B2	Remove the disabled DIMM.	Major
8545	Memory disabled.CPU0_DIMM_B3	Remove the disabled DIMM.	Major
8546	Memory disabled.CPU0_DIMM_C1	Remove the disabled DIMM.	Major
8547	Memory disabled.CPU0_DIMM_C2	Remove the disabled DIMM.	Major
8548	Memory disabled.CPU0_DIMM_C3	Remove the disabled DIMM.	Major
8549	Memory disabled.CPU0_DIMM_D1	Remove the disabled DIMM.	Major
854A	Memory disabled.CPU0_DIMM_D2	Remove the disabled DIMM.	Major
854B	Memory disabled.CPU0_DIMM_D3	Remove the disabled DIMM.	Major
854C	Memory disabled.CPU0_DIMM_E1	Remove the disabled DIMM.	Major
854D	Memory disabled.CPU0_DIMM_E2	Remove the disabled DIMM.	Major
854E	Memory disabled.CPU0_DIMM_E3	Remove the disabled DIMM.	Major
854F	Memory disabled.CPU0_DIMM_F1	Remove the disabled DIMM.	Major

Error Code	Error Message	Action message	Type
8550	Memory disabled.CPU0_DIMM_F2	Remove the disabled DIMM.	Major
8551	Memory disabled.CPU0_DIMM_F3	Remove the disabled DIMM.	Major
8552	Memory disabled.CPU0_DIMM_G1	Remove the disabled DIMM.	Major
8553	Memory disabled.CPU0_DIMM_G2	Remove the disabled DIMM.	Major
8554	Memory disabled.CPU0_DIMM_G3	Remove the disabled DIMM.	Major
8555	Memory disabled.CPU0_DIMM_H1	Remove the disabled DIMM.	Major
8556	Memory disabled.CPU0_DIMM_H2	Remove the disabled DIMM.	Major
8557	Memory disabled.CPU0_DIMM_H3	Remove the disabled DIMM.	Major
8558	Memory disabled.CPU1_DIMM_A1	Remove the disabled DIMM.	Major
8559	Memory disabled.CPU1_DIMM_A2	Remove the disabled DIMM.	Major
855A	Memory disabled.CPU1_DIMM_A3	Remove the disabled DIMM.	Major
855B	Memory disabled.CPU1_DIMM_B1	Remove the disabled DIMM.	Major
855C	Memory disabled.CPU1_DIMM_B2	Remove the disabled DIMM.	Major
855D	Memory disabled.CPU1_DIMM_B3	Remove the disabled DIMM.	Major
855E	Memory disabled.CPU1_DIMM_C1	Remove the disabled DIMM.	Major
855F (Go to 85D0)	Memory disabled.CPU1_DIMM_C2	Remove the disabled DIMM.	Major
8560	Memory encountered a Serial Presence Detection(SPD) failure.CPU0_DIMM_A1		Major
8561	Memory encountered a Serial Presence Detection(SPD) failure.CPU0_DIMM_A2		Major
8562	Memory encountered a Serial Presence Detection(SPD) failure.CPU0_DIMM_A3		Major
8563	Memory encountered a Serial Presence Detection(SPD) failure.CPU0_DIMM_B1		Major
8564	Memory encountered a Serial Presence Detection(SPD) failure.CPU0_DIMM_B2		Major
8565	Memory encountered a Serial Presence Detection(SPD) failure.CPU0_DIMM_B3		Major
8566	Memory encountered a Serial Presence Detection(SPD) failure.CPU0_DIMM_C1		Major
8567	Memory encountered a Serial Presence Detection (SPD) failure.CPU0_DIMM_C2		Major
8568	Memory encountered a Serial Presence Detection (SPD) failure.CPU0_DIMM_C3		Major
8569	Memory encountered a Serial Presence Detection(SPD) failure.CPU0_DIMM_D1		Major
856A	Memory encountered a Serial Presence Detection(SPD) failure.CPU0_DIMM_D2		Major
856B	Memory encountered a Serial Presence Detection(SPD) failure.CPU0_DIMM_D3		Major
856C	Memory encountered a Serial Presence Detection(SPD) failure.CPU0_DIMM_E1		Major
856D	Memory encountered a Serial Presence Detection(SPD) failure.CPU0_DIMM_E2		Major
856E	Memory encountered a Serial Presence Detection(SPD) failure.CPU0_DIMM_E3		Major
856F	Memory encountered a Serial Presence Detection(SPD) failure.CPU0_DIMM_F1		Major

Error Code	Error Message	Action message	Type
8570	Memory encountered a Serial Presence Detection(SPD) failure.CPU0_DIMM_F2		Major
8571	Memory encountered a Serial Presence Detection(SPD) failure.CPU0_DIMM_F3		Major
8572	Memory encountered a Serial Presence Detection(SPD) failure.CPU0_DIMM_G1		Major
8573	Memory encountered a Serial Presence Detection(SPD) failure.CPU0_DIMM_G2		Major
8574	Memory encountered a Serial Presence Detection(SPD) failure.CPU0_DIMM_G3		Major
8575	Memory encountered a Serial Presence Detection(SPD) failure.CPU0_DIMM_H1		Major
8576	Memory encountered a Serial Presence Detection(SPD) failure.CPU0_DIMM_H2		Major
8577	Memory encountered a Serial Presence Detection(SPD) failure.CPU0_DIMM_H3		Major
8578	Memory encountered a Serial Presence Detection(SPD) failure.CPU1_DIMM_A1		Major
8579	Memory encountered a Serial Presence Detection(SPD) failure.CPU1_DIMM_A2		Major
857A	Memory encountered a Serial Presence Detection(SPD) failure.CPU1_DIMM_A3		Major
857B	Memory encountered a Serial Presence Detection(SPD) failure.CPU1_DIMM_B1		Major
857C	Memory encountered a Serial Presence Detection(SPD) failure.CPU1_DIMM_B2		Major
857D	Memory encountered a Serial Presence Detection(SPD) failure.CPU1_DIMM_B3		Major
857E	Memory encountered a Serial Presence Detection(SPD) failure.CPU1_DIMM_C1		Major
857F (Go to 85E0)	Memory encountered a Serial Presence Detection(SPD) failure.CPU1_DIMM_C2		Major
85C0	Memory failed test/initialization CPU1_DIMM_C3	Remove the disabled DIMM.	Major
85C1	Memory failed test/initialization CPU1_DIMM_D1	Remove the disabled DIMM.	Major
85C2	Memory failed test/initialization CPU1_DIMM_D2	Remove the disabled DIMM.	Major
85C3	Memory failed test/initialization CPU1_DIMM_D3	Remove the disabled DIMM.	Major
85C4	Memory failed test/initialization CPU1_DIMM_E1	Remove the disabled DIMM.	Major
85C5	Memory failed test/initialization CPU1_DIMM_E2	Remove the disabled DIMM.	Major
85C6	Memory failed test/initialization CPU1_DIMM_E3	Remove the disabled DIMM.	Major
85C7	Memory failed test/initialization CPU1_DIMM_F1	Remove the disabled DIMM.	Major
85C8	Memory failed test/initialization CPU1_DIMM_F2	Remove the disabled DIMM.	Major
85C9	Memory failed test/initialization CPU1_DIMM_F3	Remove the disabled DIMM.	Major
85CA	Memory failed test/initialization CPU1_DIMM_G1	Remove the disabled DIMM.	Major
85CB	Memory failed test/initialization CPU1_DIMM_G2	Remove the disabled DIMM.	Major
85CC	Memory failed test/initialization CPU1_DIMM_G3	Remove the disabled DIMM.	Major
85CD	Memory failed test/initialization CPU1_DIMM_H1	Remove the disabled DIMM.	Major
85CE	Memory failed test/initialization CPU1_DIMM_H2	Remove the disabled DIMM.	Major
85CF	Memory failed test/initialization CPU1_DIMM_H3	Remove the disabled DIMM.	Major
85D0	Memory disabled.CPU1_DIMM_C3	Remove the disabled DIMM.	Major
85D1	Memory disabled.CPU1_DIMM_D1	Remove the disabled DIMM.	Major

Error Code	Error Message	Action message	Type
85D2	Memory disabled.CPU1_DIMM_D2	Remove the disabled DIMM.	Major
85D3	Memory disabled.CPU1_DIMM_D3	Remove the disabled DIMM.	Major
85D4	Memory disabled.CPU1_DIMM_E1	Remove the disabled DIMM.	Major
85D5	Memory disabled.CPU1_DIMM_E2	Remove the disabled DIMM.	Major
85D6	Memory disabled.CPU1_DIMM_E3	Remove the disabled DIMM.	Major
85D7	Memory disabled.CPU1_DIMM_F1	Remove the disabled DIMM.	Major
85D8	Memory disabled.CPU1_DIMM_F2	Remove the disabled DIMM.	Major
85D9	Memory disabled.CPU1_DIMM_F3	Remove the disabled DIMM.	Major
85DA	Memory disabled.CPU1_DIMM_G1	Remove the disabled DIMM.	Major
85DB	Memory disabled.CPU1_DIMM_G2	Remove the disabled DIMM.	Major
85DC	Memory disabled.CPU1_DIMM_G3	Remove the disabled DIMM.	Major
85DD	Memory disabled.CPU1_DIMM_H1	Remove the disabled DIMM.	Major
85DE	Memory disabled.CPU1_DIMM_H2	Remove the disabled DIMM.	Major
85DF	Memory disabled.CPU1_DIMM_H3	Remove the disabled DIMM.	Major
85E0	Memory encountered a Serial Presence Detection(SPD) failure.CPU1_DIMM_C3		Major
85E1	Memory encountered a Serial Presence Detection (SPD) failure. CPU1_DIMM_D1		Major
85E2	Memory encountered a Serial Presence Detection (SPD) failure.CPU1_DIMM_D2		Major
85E3	Memory encountered a Serial Presence Detection(SPD) failure.CPU1_DIMM_D3		Major
85E4	Memory encountered a Serial Presence Detection(SPD) failure.CPU1_DIMM_E1		Major
85E5	Memory encountered a Serial Presence Detection(SPD) failure.CPU1_DIMM_E2		Major
85E6	Memory encountered a Serial Presence Detection(SPD) failure.CPU1_DIMM_E3		Major
85E7	Memory encountered a Serial Presence Detection (SPD) failure.CPU1_DIMM_F1		Major
85E8	Memory encountered a Serial Presence Detection(SPD) failure.CPU1_DIMM_F2		Major
85E9	Memory encountered a Serial Presence Detection(SPD) failure.CPU1_DIMM_F3		Major
85EA	Memory encountered a Serial Presence Detection(SPD) failure.CPU1_DIMM_G1		Major
85EB	Memory encountered a Serial Presence Detection (SPD) failure. CPU1_DIMM_G2		Major
85EC	Memory encountered a Serial Presence Detection(SPD) failure.CPU1_DIMM_G3		Major
85ED	Memory encountered a Serial Presence Detection(SPD) failure.CPU1_DIMM_H1		Major
85EE	Memory encountered a Serial Presence Detection(SPD) failure.CPU1_DIMM_H2		Major
85EF	Memory encountered a Serial Presence Detection(SPD) failure.CPU1_DIMM_H3		Major
8604	POST Reclaim of non-critical NVRAM variables		Minor
8605	BIOS Settings are corrupted		Major
8606	NVRAM variable space was corrupted and has been reinitialized		Major

Error Code	Error Message	Action message	Type
8607	Recovery boot has been initiated. **Note:** The Primary BIOS image may be corrupted or the system may hang during POST. A BIOS update is required.		Fatal
A100	BIOS ACM Error		Major
A421	PCI component encountered a SERR error		Fatal
A5A0	PCI Express component encountered a PERR error		Minor
A5A1	PCI Express component encountered an SERR error		Fatal
A6A0	DXE Boot Services driver: Not enough memory available to shadow a Legacy Option ROM.	Disable OpRom at SETUP to save runtime memory.	Minor

D.1 POST Error Beep Codes

The following table lists the POST error beep codes. Prior to system video initialization, the BIOS uses these beep codes to inform users on error conditions. The beep code is followed by a user-visible code on the POST progress LEDs.

Table 50. POST Error Beep Codes

Beeps	Error Message	POST Progress Code	Description
1 short	USB device action	N/A	Short beep sounded whenever USB device is discovered in POST or inserted or removed during runtime.
3 short	Memory error	Multiple	System halted because a fatal error related to the memory was detected.
3 long and 1 short	CPU mismatch error	E5, E6	System halted because a fatal error related to the CPU family/core/cache mismatch was detected.

The integrated BMC may generate beep codes upon detection of failure conditions. Beep codes are sounded each time the problem is discovered, such as on each power-up attempt, but are not sounded continuously. Codes that are common across all Intel server boards and systems that use same generation chipset are listed in the following table. Each digit in the code is represented by a sequence of beeps whose count is equal to the digit.

Table 51. Integrated BMC Beep Codes

Code	Reason for Beep	Associated Sensors
1-5-2-1	No CPUs installed or first CPU socket is empty	CPU Missing Sensor
1-5-2-4	MSID mismatch occurs if a processor is installed into a system board that has incompatible power capabilities.	MSID Mismatch Sensor
1-5-4-2	DC power unexpectedly lost (power good dropout) – Power unit sensors report power unit failure offset.	Power fault
1-5-4-4	Power control fault (power good assertion timeout).	Power unit – soft power control failure offset
1-5-1-2	VR Watchdog Timer sensor assertion	VR Watchdog Timer
1-5-1-4	The system does not power on or unexpectedly power off and a power supply unit (PSU) is present that is an incompatible model with one or more other PSUs in the system.	PS Status

D.2 Processor Initialization Error Summary

The following table describes mixed processor conditions and actions for all Intel server boards and Intel server systems designed with the Intel® Xeon® Scalable processor family architecture. The errors fall into one of the following categories:

- **Fatal**: If the system cannot boot, POST halts and delivers the following error message to the BIOS Setup Error Manager screen:

  ```
  Unrecoverable fatal error found. System will not boot until the error is resolved
  ```

  Press **<F2>** to enter setup

  When the **<F2>** key is pressed, the error message is displayed on the BIOS Setup Error Manager screen and an error is logged to the system event log (SEL) with the POST error code.

  The "POST Error Pause" option setting in the BIOS Setup does not affect this error.

  If the system is not able to boot, the system generates a beep code consisting of three long beeps and one short beep. The system cannot boot unless the error is resolved. The faulty component must be replaced.

  The system status LED is set to a steady amber color for all fatal errors that are detected during processor initialization. A steady amber system status LED indicates that an unrecoverable system failure condition has occurred.

- **Major**: An error message is displayed to the Error Manager screen and an error is logged to the SEL. If the BIOS Setup option "Post Error Pause" is enabled, operator intervention is required to continue booting the system. If the BIOS Setup option "POST Error Pause" is disabled, the system continues to boot.

- **Minor**: An error message may be displayed to the screen or to the BIOS Setup Error Manager and the POST error code is logged to the SEL. The system continues booting in a degraded state. The user may want to replace the erroneous unit. The "POST Error Pause" option setting in the BIOS Setup does not affect this error.

Table 52. Mixed Processor Configurations Error Summary

Error	Severity	System Action when BIOS Detects the Error Condition
Processor family not identical	Fatal	• Halts at POST code `0xE6`. • Halts with three long beeps and one short beep. • Takes fatal error action (see above) and does not boot until the fault condition is remedied.
Processor model not identical	Fatal	• Logs the POST error code into the SEL. • Alerts the BMC to set the system status LED to steady amber. • Displays `0196: Processor model mismatch detected` message in the error manager. • Takes fatal error action (see above) and does not boot until the fault condition is remedied.
Processor cores/threads not identical	Fatal	• Halts at POST code `0xE5`. • Halts with three long beeps and one short beep. • Takes fatal error action (see above) and does not boot until the fault condition is remedied.
Processor cache or home agent not identical	Fatal	• Halts at POST code `0xE5`. • Halts with three long beeps and one short beep. • Takes fatal error action (see above) and does not boot until the fault condition is remedied.

Error	Severity	System Action when BIOS Detects the Error Condition
Processor frequency (speed) not identical	Fatal	If the frequencies for all processors can be adjusted to be the same: • Adjusts all processor frequencies to the highest common frequency. • Does not generate an error – this is not an error condition. • Continues to boot the system successfully. If the frequencies for all processors cannot be adjusted to be the same: • Logs the POST error code into the SEL. • Alerts the BMC to set the system status LED to steady amber. • Does not disable the processor. • Displays `0197: Processor speeds unable to synchronize` message in the error manager. • Takes fatal error action (see above) and does not boot until the fault condition is remedied
Processor Intel® UPI link frequencies not identical	Fatal	If the link frequencies for all Intel® Ultra Path Interconnect (Intel® UPI) links can be adjusted to be the same: • Adjusts all Intel® UPI interconnect link frequencies to highest common frequency. • Does not generate an error – this is not an error condition. • Continues to boot the system successfully. If the link frequencies for all Intel® UPI links cannot be adjusted to be the same: • Logs the POST error code into the SEL. • Alerts the BMC to set the system status LED to steady amber. • Does not disable the processor. • Displays `0195: Processor Intel® UPII link frequencies unable to synchronize` message in the error manager. • Takes fatal error action (see above) and does not boot until the fault condition is remedied.
Processor microcode update failed	Major	• Logs the POST error code into the SEL. • Displays `816x: Processor 0x unable to apply microcode update` message in the error manager or on the screen. • Takes major error action. The system may continue to boot in a degraded state, depending on the “POST Error Pause” setting in setup, or may halt with the POST error code in the error manager waiting for operator intervention.
Processor microcode update missing	Minor	• Logs the POST error code into the SEL. • Displays `818x: Processor 0x microcode update not found` message in the error manager or on the screen. • The system continues to boot in a degraded state, regardless of the “POST Error Pause” setting in setup.

Appendix E. Statement of Volatility

The tables in this section are used to identify the volatile and non-volatile memory components of the Intel® Server Board M50CYP2SB1U and M50CYP2SBSTD.

The tables provide the following data for each identified component.

- **Component Type**: Three types of components are on the server board assembly:
  - **Non-volatile**: Non-volatile memory is persistent and is not cleared when power is removed from the system. Non-volatile memory must be erased to clear data. The exact method of clearing these areas varies by the specific component. Some areas are required for normal operation of the server, and clearing these areas may render the server board inoperable
  - **Volatile**: Volatile memory is cleared automatically when power is removed from the system.
  - **Battery powered RAM**: Battery powered RAM is similar to volatile memory but is powered by a battery on the server board. Data in battery powered RAM is persistent until the battery is removed from the server board.
- **Size**: Size of each component in bits, kilobits (Kbits), megabits (Mbits), bytes, kilobytes (KB), or megabytes (MB).
- **Board Location**: Board location is the physical location of each component corresponding to information on the server board silkscreen.
- **User Data**: The flash components on the server board do not store user data from the operating system. No operating system level data is retained in any listed components after AC power is removed. The persistence of information written to each component is determined by its type as described in the table.

  Each component stores data specific to its function. Some components may contain passwords that provide access to that device's configuration or functionality. These passwords are specific to the device and are unique and unrelated to operating system passwords. The specific components that may contain password data are:
  - **BIOS**: The server board BIOS provides the capability to prevent unauthorized users from configuring BIOS settings when a BIOS password is set. This password is stored in BIOS flash and is only used to set BIOS configuration access restrictions.
  - **BMC**: The server board supports an Intelligent Platform Management Interface (IPMI) 2.0 conformant baseboard management controller (BMC). The BMC provides health monitoring, alerting and remote power control capabilities for the Intel server board. The BMC does not have access to operating system level data.

    The BMC supports the capability for remote software to connect over the network and perform health monitoring and power control. This access can be configured to require authentication by a password. If configured, the BMC maintains user passwords to control this access. These passwords are stored in the BMC flash.

The Intel® Server Board M50CYP2SB family includes several components that can be used to store data. A list of those components is included in the following table.

Table 53. Server Board Components

Component Type	Size	Board Location	User Data	Name
Non-Volatile	64 MB	U4	No	BIOS Flash
Non-Volatile	128 MB	U3	No	BMC Flash
Non-Volatile	UFM 1,376 Kb M9K Memory 378 Kb	U39	No	FPGA
Volatile	4Gb	U21	No	BMC SDRAM

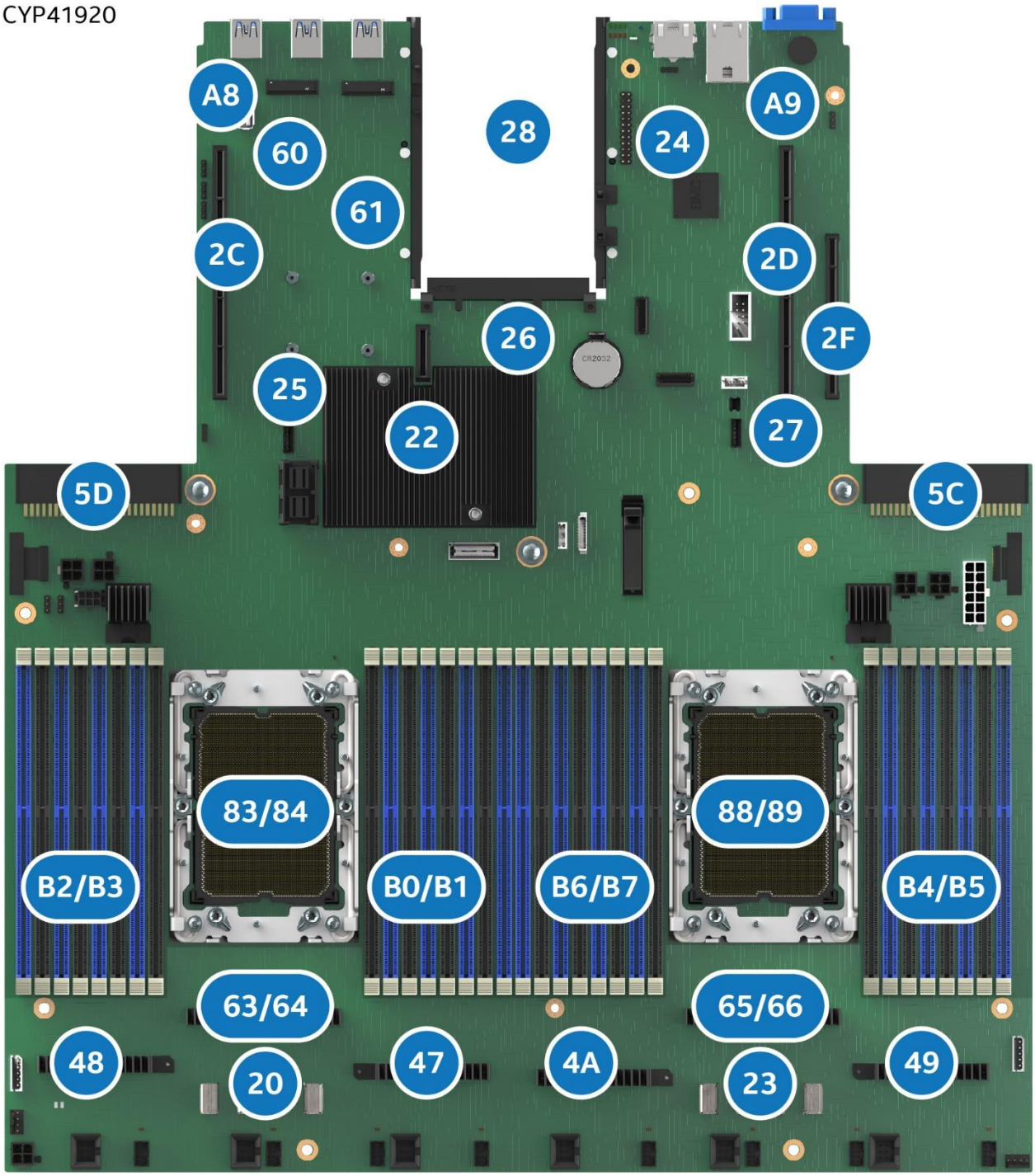
Appendix F. Connectors and Headers

Table 54. Connectors and Headers

Type	Description	Manufacturer	Manufacturer Part Number
Power	50 Pin, PSU connector	Amphenol* ICC (FCI)	10035388-102LF
Power	2x2 Pin, 12V connector for Midplane, add-in card	Lotes* Foxconn* Interconnect Technology Limited	ABA-POW-003-Y88 HM3502E-HS7
Power	2x6 Pin, 12V connector for HSBP	Lotes* Foxconn* Interconnect Technology Limited Wieson* Technologies Co., LTD	ABA-POW-025-Y06 HM3506E-HP1 G2211C888-036
IO	VGA connector	Foxconn* Interconnect Technology Limited	DZ11A57-H8R3-4F
IO	RJ45 connector	Amphenol* ICC (FCI)	RJMG2018361A1EH
IO	USB connector	Foxconn* Interconnect Technology Limited TE Connectivity (PREV Tyco Electronics	UEA11123-4HK3-4H 1932258-1
IO	Serial Connector (RJ45)	Foxconn* Interconnect Technology Limited	JMP1N07-RKM01-4H
IO	Front Panel VGA Conn	Wieson* Technologies Co., LTD	G2120C888-065H
IO	26 Pin FPC Connector for front USB panel interface	Hirose* Electric (U.S.A.), Inc.	FH34SRJ-26S-0.5SH
IO	26 Pin FPC Connector for front panel LEDs, buttons	Hirose* Electric (U.S.A.), Inc.	FH34SRJ-26S-0.5SH
Storage	SlimSAS connectors	Amphenol* FCI	U10DH3825002T
IO	4 Pin internal USB2.0 connector	Foxconn* Interconnect Technology Limited	UB01123-4BH1-4F
IO	10 Pin serial B DH-10 connector	Wieson* Technologies Co., LTD	G2120C888-019H
IO	5 Pin, I^2C connector	Joint Tech Electronic Industrial Co., Ltd.	A2506WV-05P
FAN	4 Pin, CPU FAN connector	Foxconn* Electronics Inc. Molex* Connector Corporation Wieson* Technologies Co., LTD	HF2704E-M1 47053-1000 G2366C888-007H
FAN	8 Pin, 1U FAN connector	Foxconn* Interconnect Technology Limited	HLH2047-LF00D-4H
FAN	6 Pin, 2U FAN connector	Lotes*	ABA-WAF-050-Y37
Firmware	2x6 Pin, SPI TPM, Plug, 1.27mm, Black, 10u" Au	Amphenol* FCI Wieson* Technologies Co., LTD	20021221-00312C4LF G2124C888-004H-H

Appendix G. Sensors

The following figure provides the location of the sensors on the Intel® Server Boards M50CYP2SB1U and M50CYP2SBSTD. The following table provides a list of the sensors.



Note: The numbers in the figure are hexadecimal numbers.

Figure 64. Server Board Sensor Map

Table 55. Available Sensors Monitored by the BMC

Sensor #	Sensor Name
2Bh	Hot-swap Backplane 3 Temperature (HSBP 3 Temp)
47h	P0 DIMM VR Mgn 1
48h	P0 DIMM VR Mgn 2
49h	P1 DIMM VR Mgn 1
4Ah	P1 DIMM VR Mgn 2
20h	Baseboard Temperature 1 (BB P1 VR Temp)
23h	Baseboard Temperature 2 (BB P2 VR Temp)
63h	P0 VR Ctrl Temp
64h	P0 VR Mgn
65h	P1 VR Ctrl Temp
66h	P1 VR Mgn
B0h	Processor 1 DIMM Aggregate Thermal Margin 1 (DIMM Thrm Mrgn 1)
B1h	Processor 1 DIMM Aggregate Thermal Margin 2 (DIMM Thrm Mrgn 2)
B2h	Processor 1 DIMM Aggregate Thermal Margin 3 (DIMM Thrm Mrgn 3)
B3h	Processor 1 DIMM Aggregate Thermal Margin 4 (DIMM Thrm Mrgn 4)
B4h	Processor 2 DIMM Aggregate Thermal Margin 1 (DIMM Thrm Mrgn 5)
B5h	Processor 2 DIMM Aggregate Thermal Margin 2 (DIMM Thrm Mrgn 6)
B6h	Processor 2 DIMM Aggregate Thermal Margin 3 (DIMM Thrm Mrgn 7)
B7h	Processor 2 DIMM Aggregate Thermal Margin 4 (DIMM Thrm Mrgn 8)
83h	P0 D1 DTS Th Mgn
84h	P0 D2 DTS Th Mgn
88h	P1 D1 DTS Th Mgn
89h	P1 D2 DTS Th Mgn
5Ch	Power Supply 1 Temperature (PS1 Temperature)
5Dh	Power Supply 2 Temperature (PS2 Temperature)
A8h	PHI 1 Thermal Margin (PHI 1 Margin)
A9h	PHI 2 Thermal Margin (PHI 2 Margin)

Sensor #	Sensor Name
2Ch	PCI Riser 1Temperature (Riser 1 Temp)
60h	M2 Left Margin
61h	M2 Right Margin
22h	SSB Temperature (SSB Temp)
24h	Baseboard Temperature 3 (BB BMC Temp)
25h	Baseboard Temperature 3 (BB M.2 Temp)
26h	Baseboard Temperature 5 (BB OCP Temp)
27h	Baseboard Temperature 4 (BB Rt Rear Temp)
2Dh	PCI Riser 2 Temperature (Riser 2 Temp)
2Fh	PCI Riser 3 Temperature (Riser 3 Temp)

Appendix H. Supported Intel® Server Systems

The Intel® Server Board M50CYP2SB family is designed to be integrated into high density 1U and 2U rack mount server chassis. Intel® server systems in this server board family include the Intel® Server System M50CYP2UR family and the Intel® Server System M50CYP1UR family. The sections below provide a high-level overview of the features associated with each. For additional product information, refer to the Technical Product Specification, Integration and Service Guide, Product Family Configuration Guide, and other marketing material available for each of these server families. These documents can be downloaded from the Intel website.

H.1 Intel® Server System M50CYP2UR Family

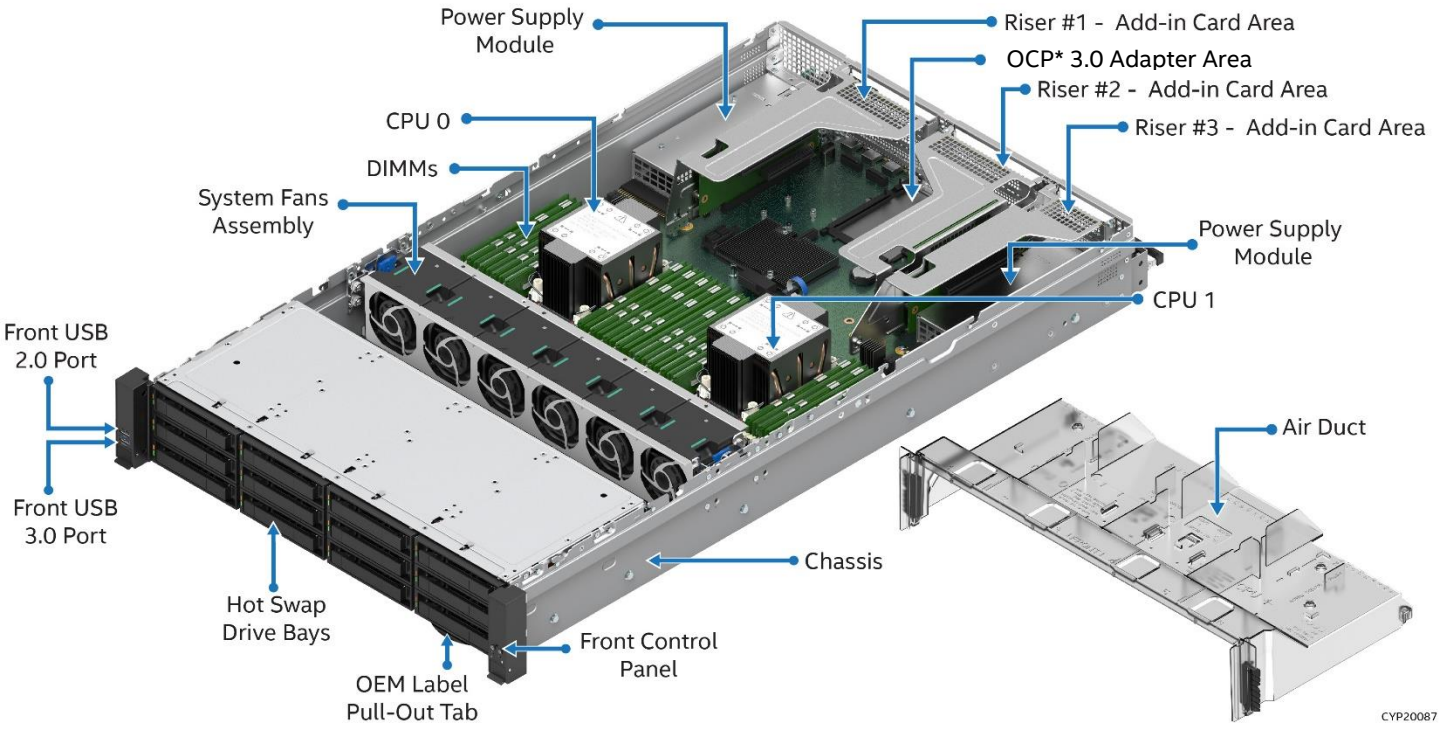


Figure 65. Intel® Server System M50CYP2UR Family

Table 56. Intel® Server System M50CYP2UR Family Features

Feature	Details
Chassis Type	2U rack mount chassis
Server Board	Intel® Server Board M50CYP2SBSTD

Processor Support	• Dual Socket-P4 LGA4189
	• Supported 3rd Gen Intel® Xeon® Scalable processor family SKUs:
	  ○ Intel® Xeon® Platinum 8300 processor
	  ○ Intel® Xeon® Gold 6300 processor
	  ○ Intel® Xeon® Gold 5300 processor
	  ○ Intel® Xeon® Silver 4300 processor
	Note: Supported 3rd Gen Intel® Xeon® Scalable processor SKUs must Not end in (H), (L), (U), or (Q). All other processor SKUs are supported.
	• UPI links: up to three at 11.2 GT/s (Platinum and Gold families) or up to two at 10.4 GT/s (Silver family)
	Note: Previous generation Intel® Xeon® processor and Intel® Xeon® Scalable processor families are not supported.

Feature	Details
Maximum Supported Processor Thermal Design Power (TDP)	• 3rd Gen Intel® Xeon® Scalable processors up to 270 W. **Note:** The maximum supported processor TDP depends on system configuration.
Chipset	• Intel® C621A Chipset (PCH)

Memory Support	• 32 DIMM slots
	  ○ 16 DIMM slots per processor, eight memory channels per processor
	  ○ Two DIMMs per channel
	• All DDR4 DIMMs must support ECC
	• Registered DDR4 (RDIMM), 3DS-RDIMM, Load Reduced DDR4 (LRDIMM), 3DS-LRDIMM
	Note: 3DS = 3 Dimensional Stacking
	• Intel® Optane™ persistent memory 200 series
	• Memory capacity
	  ○ Up to 6 TB per processor (processor SKU dependent)
	• Memory data transfer rates
	  ○ Up to 3200 MT/s at one or two DIMMs per channel (processor SKU dependent)
	• DDR4 standard voltage of 1.2 V

System Fans	• Six managed 60 mm hot swap capable system fans • Integrated fans included with each installed power supply module
Power Supply Options	The server system can have up to two power supply modules installed, providing support for the following power configurations: 1+0, 1+1 redundant power, and 2+0 combined power. Three power supply options: • AC 1300 W Titanium • AC 1600 W Titanium • AC 2100 W Platinum
Onboard Network Support	Provided by optional Open Compute Project (OCP*) adapter support. See below.
Open Compute Project* (OCP*) Adapter Support	Server board x16 PCIe* 4.0 OCP 3.0 Mezzanine connector (Small Form-Factor) slot supports the following Intel accessory options: • Dual port, RJ45, 10/1 GbE - iPC- X710T2LOCPV3 • Quad port, SFP+ DA, 4x 10 GbE - iPC- X710DA4OCPV3 • Dual Port, QSFP28 100/50/25/10 GbE - iPC- E810CQDA2OCPV3 • Dual Port, SFP28 25/10 GbE - iPC-E810XXVDA2OCPV3

Feature	Details
Riser Card Support	Concurrent support for up to three riser cards with support for up to eight PCIe* add-in cards. In the below description FH = Full Height, FL = Full Length, HL =Half Length, LP = Low Profile. **Riser Slot #1:** • Riser Slot #1 supports x32 PCIe* lanes, routed from CPU 0 • PCIe* 4.0 support for up to 64 GB/s **Riser Slot #1 supports the following Intel Riser Card options:** • Two PCIe* slot riser card supporting (one) - FH/FL double-width slot (x16 electrical, x16 mechanical) + (one) - FH/HL single-width slot (x16 electrical, x16 mechanical) iPC – CYP2URISER1DBL • Three PCIe* slot riser card supporting (one) - FH/FL single-width slot (x16 electrical, x16 mechanical) + (one) - FH/FL single-width slot (x8 electrical, x16 mechanical) + (one) - FH/HL single-width slot (x8 electrical, x8 mechanical) iPC – CYP2URISER1STD • NVMe* riser card supporting (one) – HL or FL single-width slot (x16 electrical, x16 mechanical) + (two) - x8 PCIe* NVMe* SlimSAS* connectors, each with a re-timer. iPC – CYP2URISER1RTM **Riser Slot #2:** • Riser Slot #2 supports x32 PCIe* lanes, routed from CPU 1 • PCIe* 4.0 support for up to 64 GB/s **Riser Slot #2 supports the following Intel Riser Card options:** • Two PCIe* slot riser card supporting (one) - FH/FL double-width slot (x16 electrical, x16 mechanical) + (one) - FH/HL single-width slot (x16 electrical, x16 mechanical) iPC – CYP2URISER2DBL • Three PCIe* slot riser card supporting (one) - FH/FL single-width slot (x16 electrical, x16 mechanical) + (one) - FH/FL single-width slot (x8 electrical, x16 mechanical) + (one) FH/HL single-width slot (x8 electrical, x8 mechanical) iPC – CYP2URISER2STD **Riser Slot #3:** • Riser Slot #3 supports x16 PCIe* lanes, route from CPU 1 • PCIe* 4.0 support for up to 32 GB/s **Riser Slot #3 supports the following Intel Riser Card options:** • Two PCIe* slot riser card supporting (two) LP/HL single-width slots (x16 mechanical, x8 electrical) iPC – CYP2URISER3STD • NVMe* riser card supporting (two) – PCIe* NVMe* SlimSAS* connectors with re-timers iPC – CYPRISER3RTM

PCIe* NVMe* Support	• Support for up to 10 PCIe* NVMe* Interconnects
	  ○ Eight server board SlimSAS* connectors, four per processor
	  ○ Two M.2 NVMe/SATA connectors
	• Additional NVMe* support through select Riser Card options (See Riser Card Support)
	• Intel® Volume Management Device (Intel® VMD) 2.0 support
	• Intel® Virtual RAID on CPU 7.5 (Intel® VROC 7.5) support using one of the three types of VROC keys (available as an Intel accessory option)

Video Support	• Integrated 2D video controller • 128 MB of DDR4 video memory • One VGA DB-15 external connector in the back

Onboard SATA Support	• 10 x SATA III ports (6 Gb/s, 3 Gb/s and 1.5 Gb/s transfer rates supported)
	  ○ Two M.2 connectors – SATA/PCIe*
	  ○ Two 4-port Mini-SAS HD (SFF-8643) connectors

USB Support	• Three USB 3.0 connectors on the back panel • One USB 3.0 and one USB 2.0 connector on the front panel • One USB 2.0 internal Type-A connector
Serial Support	• One external RJ-45 Serial Port A connector on the back panel • One internal DH-10 Serial Port B header for optional front or rear serial port support. The port follows DTK pinout specifications.
Front Drive Bay Options	• 8 x 2.5” SAS/SATA/NVMe* hot swap drive bays • 16 x 2.5” SAS/SATA/NVMe* hot swap drive bays • 24 x 2.5” SAS/SATA/NVMe* hot swap drive bays • 12 x 3.5” SAS/SATA hot swap drive bays (supports up to 4 NVMe* drives)

Feature	Details
Server Management	• Integrated Baseboard Management Controller (BMC) • Intelligent Platform Management Interface (IPMI) 2.0 compliant • Redfish* compliant • Support for Intel® Data Center Manager (DCM) • Support for Intel® Server Debug and Provisioning Tool (SDPTool) • Support for Intel® Server Management Software • Dedicated server board RJ45 1 GbE management port • Light Guided Diagnostics
System Configuration and Recovery Jumpers	• BIOS load defaults • BIOS Password clear • Intel® Management Engine firmware force update Jumper • BMC force update • BIOS_SVN Downgrade • BMC_SVN Downgrade For more information, see the *Intel® Server Board M50CYP2SB Family Technical Product Specification (TPS).*
Security Support	• Intel® Platform Firmware Resilience (Intel® PFR) technology with an I^2C interface • Intel® Software Guard Extensions (Intel® SGX) • Intel® CBnT – Converged Intel® Boot Guard and Trusted Execution Technology (Intel® TXT) • Intel® Total Memory Encryption (Intel® TME) • Trusted platform module 2.0 (Rest of World) – iPC J33567-151 (accessory option) • Trusted platform module 2.0 (China Version) – iPC J12350-150 (accessory option)
Supported Rack Mount Kit Accessory Options	**CYPHALFEXTRAIL** –Value Rack Mount Rail Kit **CYPFULLEXTRAIL** – Premium Rail Kit with cable management arm (CMA) support **AXXCMA2** – Cable Management Arm (supports **CYPFULLEXTRAIL** only)
BIOS	Unified Extensible Firmware Interface (UEFI)-based BIOS (legacy boot not supported)

H.2 Intel® Server System M50CYP1UR Family

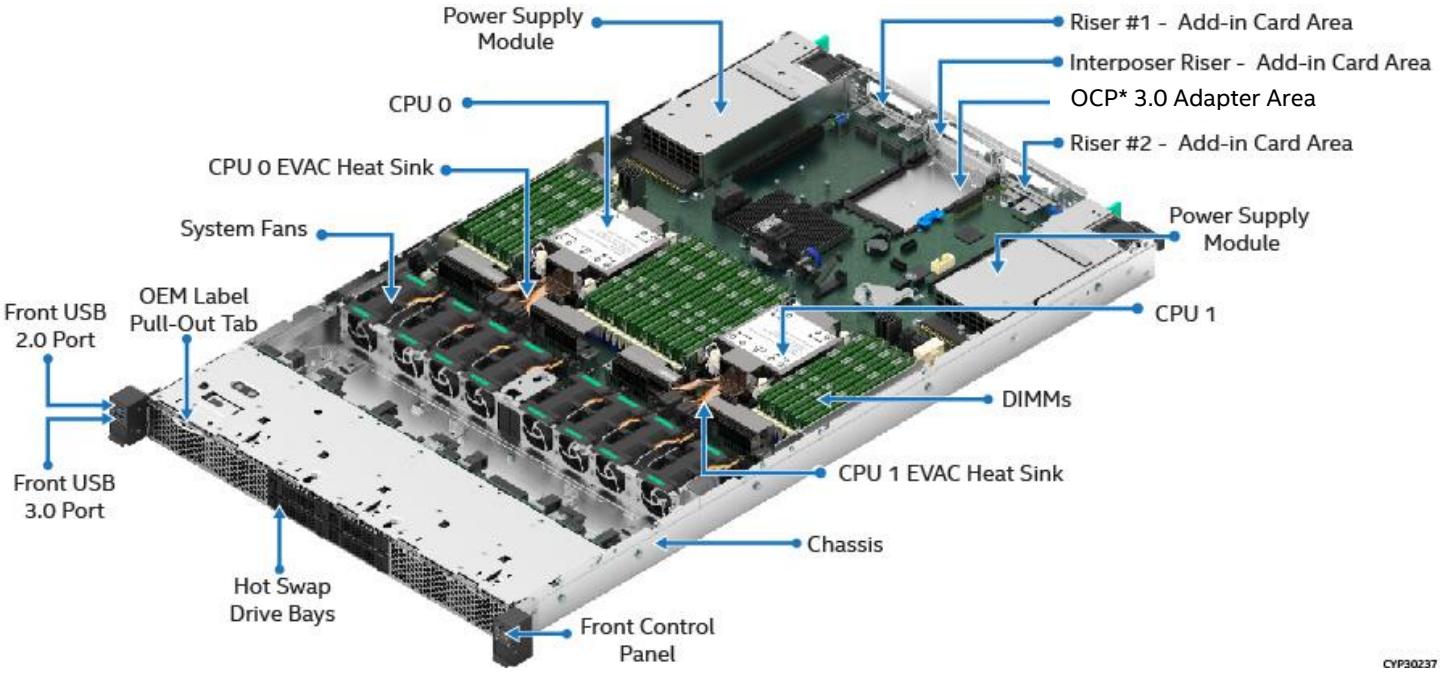


Figure 66. Intel® Server System M50CYP1UR Family

Table 57. Intel® Server System M50CYP1UR Family Features

Feature	Details
Chassis Type	1U rack mount chassis
Server Board	Intel® Server Board M50CYP2SB1U

Processor Support	• Dual Socket-P4 LGA4189
	• Supported 3rd Gen Intel® Xeon® Scalable processor family SKUs:
	  ○ Intel® Xeon® Platinum 8300 processor
	  ○ Intel® Xeon® Gold 6300 processor
	  ○ Intel® Xeon® Gold 5300 processor
	  ○ Intel® Xeon® Silver 4300 processor
	Note: Supported 3rd Gen Intel® Xeon® Scalable processor SKUs must Not end in (H), (L), (U), or (Q). All other processor SKUs are supported.
	• UPI links: up to three at 11.2 GT/s (Platinum and Gold families) or up to two at 10.4 GT/s (Silver family)
	Note: Previous generation Intel® Xeon® processor and Intel® Xeon® Scalable processor families are not supported.

Maximum Supported Processor Thermal Design Power (TDP)	• 3rd Gen Intel® Xeon® Scalable processors up to 270 W. **Note:** The maximum supported processor TDP depends on system configuration.
Chipset	• Intel® C621A Chipset (PCH)

Memory Support	• 32 DIMM slots
	  ○ 16 DIMM slots per processor, eight memory channels per processor
	  ○ Two DIMMs per channel
	• All DDR4 DIMMs must support ECC
	• Registered DDR4 (RDIMM), 3DS-RDIMM, Load Reduced DDR4 (LRDIMM), 3DS-LRDIMM
	Note: 3DS = 3 Dimensional Stacking
	• Intel® Optane™ persistent memory 200 series
	• Memory capacity
	  ○ Up to 6 TB per processor (processor SKU dependent)
	• Memory data transfer rates
	  ○ Up to 3200 MT/s at one or two DIMMs per channel (processor SKU dependent)
	• DDR4 standard voltage of 1.2V

System Fans	• Eight managed 40 mm hot swap capable system fans • Integrated fans included with each installed power supply module **Note:** System fan redundancy is supported on specific system configurations.
Power Supply Options	The server system can have up to two power supply modules installed, supporting the following power configurations: 1+0, 1+1 redundant power, and 2+0 combined power. Three power supply options: • AC 1300 W Titanium • AC 1600 W Titanium
Server Board Network Support	See optional Open Compute Project (OCP*) adapter support below.
Open Compute Project* (OCP*) Adapter Support	Onboard x16 PCIe* 4.0 OCP 3.0 Mezzanine connector (Small Form-Factor) supports the following Intel accessory options: • Dual port, RJ45, 10/1 GbE, - iPC- X710T2LOCPV3 • Quad port, SFP+ DA, 4x 10 GbE - iPC- X710DA4OCPV3 • Dual Port, QSFP28 100/50/25/10 GbE - iPC- E810CQDA2OCPV3 • Dual Port, SFP28 25/10 GbE - iPC-E810XXVDA2OCPV3

Feature	Details
Riser Card Support	Concurrent support for up to four riser cards, including one PCIe Interposer riser card with support for up to three PCIe* add-in cards. In the below description HL = Half Length, LP = Low Profile. **Riser Slot #1:** • Riser Slot #1 supports x16 PCIe* lanes routed from CPU 0 • PCIe* 4.0 support for up to 32 GB/s **Riser Slot #1 supports the following Intel Riser Card option:** • One PCIe* slot Riser card supporting (one) – LP/HL, single-width slot (x16 electrical, x16 mechanical) iPC – CYP1URISER1STD **Riser Slot #2:** • Riser Slot #2 supports X24 PCIe* lanes routed from CPU 1 • PCIe* 4.0 support for up to 32 GB/s **Riser Slot #2 supports the following Intel Riser Card options:** • One PCIe* slot Riser card supporting (one) – LP/HL, single-width slot (x16 electrical, x16 mechanical) iPC – CYP1URISER2STD • NVMe* Riser card supporting (one) – LP/HL, single-width slot (x16 electrical, x16 mechanical) + (one) - x8 PCIe* NVMe* SlimSAS* connector with re-timer. Included in iPC – CYP1URISER2KIT **PCIe* Interposer Riser Slot (requires PCIe* NVMe* riser card in Riser Slot #2)** • PCIe* Interposer Riser Slot supports the PCIe* interposer riser card as an accessory option. This card supports one PCIe* add-in card (x8 electrical, x8 mechanical). The PCIe* interposer riser card can be used only when it is connected to the PCIe* NVMe* riser card in Riser Slot #2. The interposer card uses x8 PCIe* data lanes routed from the PCIe* SlimSAS* connector on the PCIe* NVMe* riser card. The Intel accessory kit includes the PCIe* interposer riser card, PCIe* NVMe* riser card, and PCIe* interposer cable. iPC – CYP1URISER2KIT **Riser Slot #3:** • Riser Slot #3 supports x16 PCIe* lanes routed from CPU 1 • PCIe* 4.0 support for up to 32 GB/s **Riser Slot #3 supports the following Intel Riser Card option:** • NVMe* riser card supporting (two) – PCIe* NVMe* SlimSAS* connectors iPC – CYPRISER3RTM **Note:** Riser Slot #3 does not support add-In cards

PCIe* NVMe* Support	• Support for up to 10 PCIe* NVMe* Interconnects
	  ○ Eight server board SlimSAS* connectors, four per processor
	  ○ Two M.2 NVMe/SATA connectors
	• Additional NVMe* support through select Riser Card options (See Riser Card Support)
	• Intel® Volume Management Device 2.0 (Intel® VMD 2.0) support
	• Intel® Virtual RAID on CPU 7.5 (Intel® VROC 7.5) support using one of the three types of VROC keys (available as an Intel accessory option)

Video Support	• Integrated 2D video controller • 128 MB of DDR4 video memory • One VGA DB-15 external connector in the back

Server Board SATA Support	• 10 x SATA III ports (6 Gb/s, 3 Gb/s and 1.5 Gb/s transfer rates supported)
	  ○ Two M.2 connectors – SATA / PCIe*
	  ○ Two 4-port Mini-SAS HD (SFF-8643) connectors

USB Support	• Three USB 3.0 connectors on the back panel • One USB 3.0 and one USB 2.0 connector on the front panel • One USB 2.0 internal Type-A connector
Serial Support	• One external RJ-45 Serial Port A connector on the back panel • One internal DH-10 Serial Port B header for optional front or rear serial port support. The port follows the DTK pinout specifications.
Front Drive Bay Options	• 4 x 2.5” SAS/SATA/NVMe* hot swap drive bays • 12 x 2.5” SAS/SATA/NVMe* hot swap drive bays

Feature	Details
Server Management	• Integrated Baseboard Management Controller (BMC) • Intelligent Platform Management Interface (IPMI) 2.0 compliant • Redfish* compliant • Support for Intel® Data Center Manager (DCM) • Support for Intel® Server Debug and Provisioning Tool (SDPTool) • Dedicated server board RJ45 1 GbE management port • Light Guided Diagnostics
System Configuration and Recovery Jumpers	• BIOS load defaults • BIOS Password clear • Intel® Management Engine firmware force update Jumper • BMC force update • BIOS_SVN Downgrade • BMC_SVN Downgrade For more information, see the *Intel® Server Board M50CYP2SB Family* Technical Product Specification (TPS).
Security Support	• Intel® Platform Firmware Resilience (Intel® PFR) technology with an I^2C interface • Intel® Software Guard Extensions (Intel® SGX) • Intel® CBnT – Converged Intel® Boot Guard and Trusted Execution Technology (Intel® TXT) • Intel® Total Memory Encryption (Intel® TME) • Trusted platform module 2.0 (Rest of World) – iPC J33567-151 (accessory option) • Trusted platform module 2.0 (China Version) – iPC J12350-150 (accessory option)
Supported Rack Mount Kit Accessory Options	• **CYPHALFEXTRAIL** –Value Rack Mount Rail Kit • **CYPFULLEXTRAIL** – Premium Rail Kit with cable management arm (CMA) support • **AXXCMA2** – Cable Management Arm (supports **CYPFULLEXTRAIL** only)
BIOS	Unified Extensible Firmware Interface (UEFI)-based BIOS (legacy boot not supported)

Appendix I. Regulatory Information

This product has been evaluated and certified as Information Technology Equipment (ITE), which may be installed in offices, schools, computer rooms, and similar commercial type locations. The suitability of this product for other product certification categories and/or environments (such as: medical, industrial, telecommunications, NEBS, residential, alarm systems, test equipment, and so on), other than an ITE application, will require further evaluation and may require additional regulatory approvals.

Intel has verified that all L3, L6, and L9 server products[1] **as configured and sold by Intel** to its customers comply with the requirements for all regulatory certifications defined in the following table. It is the Intel customer's responsibility to ensure their final server system configurations are tested and certified to meet the regulatory requirements for the countries to which they plan to ship and or deploy server systems into.

	Intel® Server Board M50CYP2SB Family	Intel® Server System M50CYP2UR Family	Notes
	"Coyote Pass"	2U "Coyote Pass"	Intel Project Code Name
	L3 Board	L6/L9 System	Product integration level
	M50CYP	M500002UR M500001UR	Product family identified on certification
Regulatory Certification			
RCM DoC Australia & New Zealand	✓	✓	
CB Certification & Report (International - report to include all CB country national deviations)	✓	✓	
China CCC Certification	○	○	Out of CCC Scope
CU Certification (Russia/Belarus/Kazakhstan)	○	✓	
Europe CE Declaration of Conformity	✓	✓	
FCC Part 15 Emissions Verification (USA & Canada)	✓	✓	
Germany GS Certification	○	✓	
India BIS Certification	○	●	Only L9 at MSL
International Compliance – CISPR32 & CISPR24	✓	✓	
Japan VCCI Certification	○	✓	
Korea KC Certification	✓	✓	
Mexico Certification	○	✓	
NRTL Certification (USA&Canada)	✓	✓	
South Africa Certification	○	✓	
Taiwan BSMI Certification	✓	✓	
Ukraine Certification	○	✓	

Table Key

Not Tested / Not Certified	○
Tested / Certified – Limited OEM SKUs only	●
Testing / Certification (Planned)	(Date)
Tested / Certified	✓

[1] An L9 system configuration is a power-on ready server system with NO operating system installed.
An L6 system configuration requires additional components to be installed in order to make it power-on ready. L3 are component building block options that require integration into a chassis to create a functional server system.

EU Directive 2019/424 (Lot 9)

Beginning on March 1, 2020, an additional component of the European Union (EU) regulatory CE marking scheme, identified as EU Directive 2019/424 (Lot 9), will go into effect. After this date, all new server systems shipped into or deployed within the EU must meet the full CE marking requirements including those defined by the additional EU Lot 9 regulations.

Intel has verified that all L3, L6, and L9 server products[2] **as configured and sold by Intel** to its customers comply with the full CE regulatory requirements for the given product type, including those defined by EU Lot 9. It is the Intel customer's responsibility to ensure their final server system configurations are SPEC® SERT™ tested and meet the new CE regulatory requirements.

Visit the following website for additional EU Directive 2019/424 (Lot9) information:
https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32019R0424

In compliance with the EU Directive 2019/424 (Lot 9) materials efficiency requirements, Intel makes available all necessary product collaterals as identified below:

- **System Disassembly Instructions**
  - *Intel® Server System M50CYP2UR Family System Integration and Service Guide*
    https://www.intel.com/content/www/us/en/support/products/200321.html
  - *Intel® Server System M50CYP1UR Family System Integration and Service Guide*
    https://www.intel.com/content/www/us/en/support/products/200321.html

- **Product Specifications**
  - *Intel® Server Board M50CYP2SB Family Technical Product Specification* (This document)
    https://www.intel.com/content/www/us/en/support/products/200321.html
  - *Intel® Server System M50CYP2UR Family Technical Product Specification*
    https://www.intel.com/content/www/us/en/support/products/200321.html
  - *Intel® Server System M50CYP1UR Family Technical Product Specification*
    https://www.intel.com/content/www/us/en/support/products/200321.html

- **System BIOS/Firmware and Security Updates – Intel® Server Board M50CYP2SB family**
  - System Update Package (SUP) – uEFI only
    http://downloadcenter.intel.com

- **Intel® Solid State Drive (SSD) Secure Data Deletion and Firmware Updates**
  - Note: for system configurations that may be configured with an Intel SSD
  - Intel® Solid State Drive Toolbox
    https://downloadcenter.intel.com/product/35125/Memory-and-Storage

- **Intel® RAID Controller Firmware Updates and other support collaterals**
  - Note: for system configurations that may be configured with an Intel® RAID Controller
    https://www.intel.com/content/www/us/en/support/products/43732/server-products/raid-products.html

[2] An L9 system configuration is a power-on ready server system with NO operating system installed.
An L6 system configuration requires additional components to be installed in order to make it power-on ready. L3 are component building block options that require integration into a chassis to create a functional server system

Appendix J. Glossary

Term	Definition
ACPI	Advanced Configuration and Power Interface
ARP	Address Resolution Protocol
ASHRAE	American Society of Heating, Refrigerating and Air-Conditioning Engineers
BBS	BIOS Boot Selection
BMC	Baseboard Management Controller
BIOS	Basic Input/Output System
CFM	Cubic Feet per Minute
CLST	Closed Loop System Throttling
CMOS	Complementary Metal-oxide-semiconductor
CPU	Central Processing Unit
DDR4	Double Data Rate 4
DHCP	Dynamic Host Configuration Protocol
DIMM	Dual In-line Memory Module
DPC	DIMMs per Channel
DR	Dual Rank
EDS	External Design Specification
EFI	Extensible Firmware Interface
FP	Front Panel
FRB	Fault Resilient Boot
FRU	Field Replaceable Unit
GPGPU	General Purpose Graphic Processing Unit
GPIO	General Purpose Input/Output
GUI	Graphical User Interface
I²C	Inter-integrated Circuit bus
IMC	Integrated Memory Controller
IIO	Integrated Input/Output
iPC	Intel Product Code
IPMI	Intelligent Platform Management Interface
LED	Light Emitting Diode
LFM	Linear Feet per Minute – Airflow measurement
LPC	Low-pin Count
LRDIMM	Load Reduced DIMM
LSB	Least Significant Bit
MSB	Most Significant Bit
MKTME	Multi-key Total Memory Encryption

Term	Definition
MLE	Measured Launched Environment
MM	Memory Mode
MRC	Memory Reference Code
MTBF	Mean Time Between Failure
NAT	Network Address Translation
NIC	Network Interface Controller
NMI	Non-maskable Interrupt
NTB	Non-Transparent Bridge
OCuLink	Optical Copper Link
OEM	Original Equipment Manufacturer
OCP*	Open Compute Project*
OR	Oct Rank
OTP	Over Temperature Protection
OVP	Over-voltage Protection
PCH	Peripheral Controller Hub
PCI	Peripheral Component Interconnect
PCB	Printed Circuit Board
PCIe*	Peripheral Component Interconnect Express*
PFC	Power Factor Correction
PHM	Processor Heat sink Module
PMBus	Power Management Bus
PMem	Persistent Memory Module
POST	Power-on Self-Test
PSU	Power Supply Unit
PWM	Pulse Width Modulation
QR	Quad (8) Rank
RAID	Redundant Array of Independent Disks
RAM	Random Access Memory
RAS	Reliability, Availability, and Serviceability
RCiEP	Root Complex Integrated Endpoint
RDIMM	Registered DIMM
RMCP	Remote Management Control Protocol
ROC	RAID On Chip
SAS	Serial Attached SCSI
SATA	Serial Advanced Technology Attachment
SEL	System Event Log
SCA	Single Connector Attachment
SCSI	Small Computer System Interface

Term	Definition
SDR	Sensor Data Record
SFF	Small Form Factor
SFP	Small Form-factor Pluggable
SFUP	System Firmware Update Package
SMBus	System Management Bus
SMTP	Simple Mail Transfer Protocol
SNMP	Simple Network Management Protocol
SOL	Serial-over-LAN
SR	Single Rank
SSD	Solid State Device
TCG	Trusted Computing Group
TDP	Thermal Design Power
TPM	Trusted Platform Module
TPS	Technical Product Specification
Intel® TXT	Intel® Trusted Execution Technology
Intel® VMD	Intel® Volume Management Device
UEFI	Unified Extensible Firmware Interface
VLSI	Very Large Scale Integration
VSB	Voltage Standby
Intel® VROC	Intel® Virtual RAID on CPU
Intel® VT-d	Intel® Virtualization Technology for Directed I/O
Intel® VT-x	Intel® Virtualization Technology for IA-32, Intel® 64 and Intel® Architecture