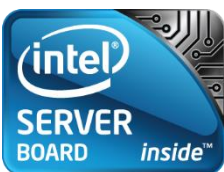# Intel® Server Board S1200SP Family

## *Technical Product Specification*

**Revision 1.0**

**November, 2015**

## *Revision History*

| Date | Revision Number | Modifications |
|---|---|---|
| Nov. 2015 | 1.0 | Initial version |
|  |  |  |

# *Disclaimers*

INFORMATION IN THIS DOCUMENT IS PROVIDED IN CONNECTION WITH INTEL PRODUCTS. NO LICENSE, EXPRESS OR IMPLIED, BY ESTOPPEL OR OTHERWISE, TO ANY INTELLECTUAL PROPERTY RIGHTS IS GRANTED BY THIS DOCUMENT. EXCEPT AS PROVIDED IN INTEL'S TERMS AND CONDITIONS OF SALE FOR SUCH PRODUCTS, INTEL ASSUMES NO LIABILITY WHATSOEVER AND INTEL DISCLAIMS ANY EXPRESS OR IMPLIED WARRANTY, RELATING TO SALE AND/OR USE OF INTEL PRODUCTS INCLUDING LIABILITY OR WARRANTIES RELATING TO FITNESS FOR A PARTICULAR PURPOSE, MERCHANTABILITY, OR INFRINGEMENT OF ANY PATENT, COPYRIGHT OR OTHER INTELLECTUAL PROPERTY RIGHT.

A "Mission Critical Application" is any application in which failure of the Intel Product could result, directly or indirectly, in personal injury or death. SHOULD YOU PURCHASE OR USE INTEL'S PRODUCTS FOR ANY SUCH MISSION CRITICAL APPLICATION, YOU SHALL INDEMNIFY AND HOLD INTEL AND ITS SUBSIDIARIES, SUBCONTRACTORS AND AFFILIATES, AND THE DIRECTORS, OFFICERS, AND EMPLOYEES OF EACH, HARMLESS AGAINST ALL CLAIMS COSTS, DAMAGES, AND EXPENSES AND REASONABLE ATTORNEYS' FEES ARISING OUT OF, DIRECTLY OR INDIRECTLY, ANY CLAIM OF PRODUCT LIABILITY, PERSONAL INJURY, OR DEATH ARISING IN ANY WAY OUT OF SUCH MISSION CRITICAL APPLICATION, WHETHER OR NOT INTEL OR ITS SUBCONTRACTOR WAS NEGLIGENT IN THE DESIGN, MANUFACTURE, OR WARNING OF THE INTEL PRODUCT OR ANY OF ITS PARTS.

Intel may make changes to specifications and product descriptions at any time, without notice. Designers must not rely on the absence or characteristics of any features or instructions marked "reserved" or "undefined". Intel reserves these for future definition and shall have no responsibility whatsoever for conflicts or incompatibilities arising from future changes to them. The information here is subject to change without notice. Do not finalize a design with this information.

The products described in this document 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.

Contact your local Intel sales office or your distributor to obtain the latest specifications and before placing your product order.

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

Intel and Xeon are trademarks or registered trademarks of Intel Corporation.

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

## *Table of Contents*

# *List of Figures*

## List of Tables

**< This page intentionally left blank. >**

# 1.　　Introduction

This *Technical Product Specification* (TPS) provides board specific information detailing the features, functionality, and high-level architecture of the Intel® Server Board S1200SP family.

Design-level information related to specific server board components and subsystems can be obtained by ordering *External Product Specifications* (EPS) or *External Design Specifications* (EDS) related to this server generation. EPS and EDS documents are made available under NDA with Intel® and must be ordered through your local Intel® representative. See the Reference Documents section for a list of available documents.

## 1.1　　Chapter Outline

This document is divided into the following chapters:

- Chapter 1 – Introduction
- Chapter 2 – Overview
- Chapter 3 – Functional Architecture
- Chapter 4 – System Security
- Chapter 5 – Intel® Technology Support
- Chapter 6 – Platform Management Functional Overview
- Chapter 7 – Advanced Management Feature Support (RMM4)
- Chapter 8 – On-board Connector/Header Overview
- Chapter 9 – BIOS Setup Interface
- Chapter 10 – Jumper Blocks
- Chapter 11 – Intel® Light Guided Diagnostics
- Chapter 12 – Environmental Limits Specifications
- Chapter 13 – Server Board Power Distribution
- Appendix A – Integration and Usage Tips
- Appendix B – Integrated BMC Sensor Tables
- Appendix C – POST Code Diagnostic LED Decoder
- Appendix D – POST Code Errors
- Appendix E – Supported Intel® Server Chassis
- Glossary
- Reference Documents

## 1.2    Server Board Use Disclaimer

Intel® Corporation server boards support add-in peripherals and contain a number of high-density Very Large Scale Integration (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 will meet 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 their specific application and environmental conditions. Intel® Corporation cannot be held responsible if components fail or the server board does not operate correctly when used outside any of their published operating or non-operating limits.

# 2.   Overview

The Intel® Server Board S1200SP product family consist of S1200SPS and S1200SPL. The server boards are monolithic printed circuit boards (PCBs) with features designed to support the pedestal or rack server markets. These server boards are designed to support the Intel® Xeon® processor E3-1200 V5 product family. Previous generation Intel® Xeon® processors are not supported. Many of the features and functions of these three server boards are common. A board will be identified by name when a described feature or function is unique to it.

## 2.1   Intel® Server Board S1200SP Family Feature Set

**Table 1. Intel® Server Board S1200SP Feature Set**

| | S1200SPL | S1200SPS |
|---|---|---|
| Form Factor | MicroATX 9.6"x9.6" compliant form factor | |
| Processor | ▪ Support for one Intel® Xeon® E3-1200 V5 processor in an LGA 1151 Socket H4 package with Thermal Design Power up to 80W<br>▪ S1200SPL supports Intel® Xeon® processor E3-1200 V5 processor graphics (GT2 or 4+2), S1200SPS supports Intel® Xeon® processor E3-1200 V5 without processor graphics (GT0 or 4+0).<br>▪ 8 GT/s point-to-point DMI 3.0 interface to PCH | |
| Chipset | Intel® C236 Platform Controller Hub (PCH) chipset | Intel® C232 Platform Controller Hub (PCH) chipset |
| Memory | ▪ Two memory channels, four memory DIMMs (Two memory DIMMs per channel)<br>▪ Support for 2133 MT/s Unbuffered (UDIMM DDR4 ECC memory)<br>▪ No support for RDIMMs<br>▪ No support for SODIMMs<br>▪ No support for mixing ECC and non-ECC UDIMMs | |
| Max Memory | 64GB | 64GB |
| Add-in PCI Express* Slots and Module Connectors Number | 4<br>See Note. | 3<br>See Note. |
| Add-in PCI Express* Slots and Module Connectors Configuration | Slot 6: PCI Express* Gen3 x 8 electrical with 16 physical connectors, from processor | Slot 6: PCI Express* Gen3 x 8 electrical with 16 physical connectors, from processor |
| | Slot 5: PCI Express* Gen3 x 4 electrical with 8 physical connectors, from PCH | Slot 5: PCI Express* Gen3 x 4 electrical with 8 physical connectors, from PCH |
| | Slot 4: PCI Express* Gen3 x 8 electrical with 8 physical connectors, from processor | Slot 4: PCI Express* Gen3 x 8 electrical with 8 physical connectors, from processor |
| | PCI Express* Gen3 x 4 SAS module connector, from PCH | |
| Add-in PCI Express* Slots and Module Connectors Configuration | PCI Express* Gen3 x8 electrical with x16 physical connector, from processor | PCI Express* Gen3 x8 electrical with x16 physical connector, from processor |
| | PCI Express* Gen3 x4 electrical with x8 physical connector, from PCH | PCI Express* Gen3 x4 electrical with x8 physical connector, from PCH |
| | PCI Express* Gen3 x8 electrical with x8 physical connector, from processor | PCI Express* Gen3 x8 electrical with x8 physical connector, from processor |

| | S1200SPL | S1200SPS |
|---|---|---|
| | PCI Express* Gen3 x4 SAS module connector, from PCH | |
| Ethernet | Two Gigabit Ethernet Ports through the two Intel® Ethernet Controller I210 PHYs | Two Gigabit Ethernet Ports through the two Intel® Ethernet Controller I210 PHYs |
| Storage | <ul><li>8x SATA connectors at 6Gbps</li><li>2x SGPIO</li><li>1x HSBP I$^2$C</li><li>1x SATADOM connector (SATA port 4)</li></ul> | <ul><li>6x SATA connectors at 6Gbps</li><li>1x SGPIO</li><li>1x HSBP I$^2$C</li><li>1x SATADOM connector (SATA port 4)</li></ul> |
| SSD | 1x 75 pin connector for M.2 SATA SSD (2242 form factor) | N/A |
| SW RAID | <ul><li>Intel® RSTe 4.x SW RAID through onboard SATA connectors provides SATA RAID 0/1/10/5.</li><li>Intel® Embedded Server RAID Technology II through onboard SATA connectors provides SATA RAID 0/1/10 and optional RAID 5 support provided by the Intel® RAID Activation Key RKSATA8R5.</li></ul> | |
| Video | <ul><li>Display Port from CPU</li><li>Integrated 2D video controller in BMC</li></ul> | <ul><li>Integrated 2D video controller in BMC</li></ul> |
| Video Connector | <ul><li>1x Display Port</li><li>1x DB-15 video connector</li></ul> | <ul><li>1x DB-15 video connector</li></ul> |
| ISM | <ul><li>BMC</li><li>IPMI 2.0</li><li>1x on-board dedicated RMM4 NIC connector</li></ul> | <ul><li>BMC</li><li>IPMI 2.0</li></ul> |
| | Intel® Remote Management Module 4 Lite solutions | N/A |
| TPM | TPM 1.2 based on LPC | N/A |
| USB | <ul><li>2x USB 3.0 ports at the back of the board</li><li>2x USB 2.0 ports at the back of the board</li><li>One 2x10 pin USB 3.0 header, providing front panel support for two USB ports respectively</li><li>One 2x5 pin USB 2.0 header, providing front panel support for two USB ports respectively</li><li>1x internal Type-A USB 2.0 port</li></ul> | <ul><li>2x USB 3.0 ports at the back of the board</li><li>2x USB 2.0 ports at the back of the board</li><li>One 2x5 pin USB 2.0 header, providing front panel support for two USB ports respectively</li><li>1x internal Type-A USB 2.0 port</li></ul> |

*Note: The server board S1200SPL and S1200SPS support full height full length PCIe* cards. See the following table for the limitations when the server boards is installed in server chassis P4000XXSFDR.*

## Table 2. Limiting Conditions of PCIe* Card Form Factor

| PCIe Slot # | Conditions for full height and half length card | Conditions for full height and ¾ length card |
|---|---|---|

| 4 | Mezzanine SAS module is installed or SATA port 4-7 are occupied. | Mezzanine slot and SATA port 4-7 are not occupied. |
|---|---|---|
| 5 | Mezzanine SAS module is installed or SATA port 0-3 are occupied. | Mezzanine slot and SATA port 0-3 are not occupied. |
| 6 | Mezzanine SAS module is installed. | Mezzanine slot is not occupied. |

## 2.2    Server Board Layout



**Figure 1. Intel® Server Board S1200SP Layout (S1200SPL)**

## 2.2.1       Server Board Connector and Component Layout

Each connector and major component is identified in the figure below.
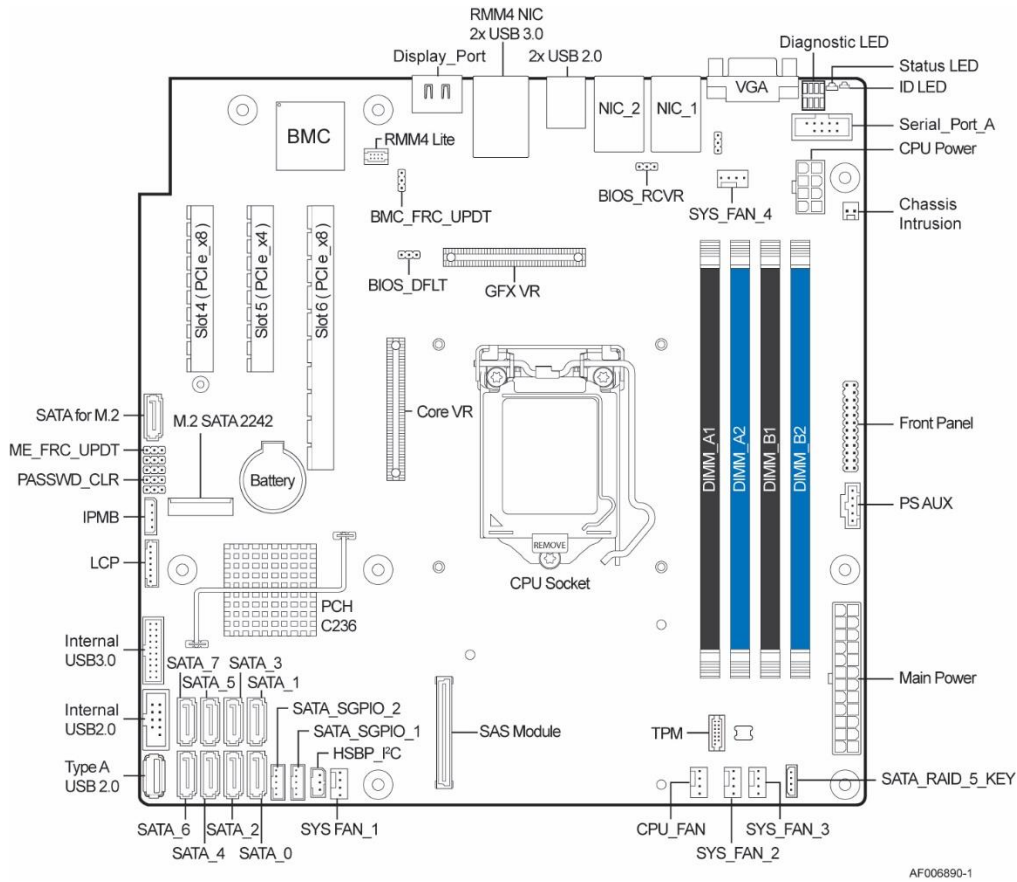


**Figure 2. Intel® Server Board S1200SPL Layout**
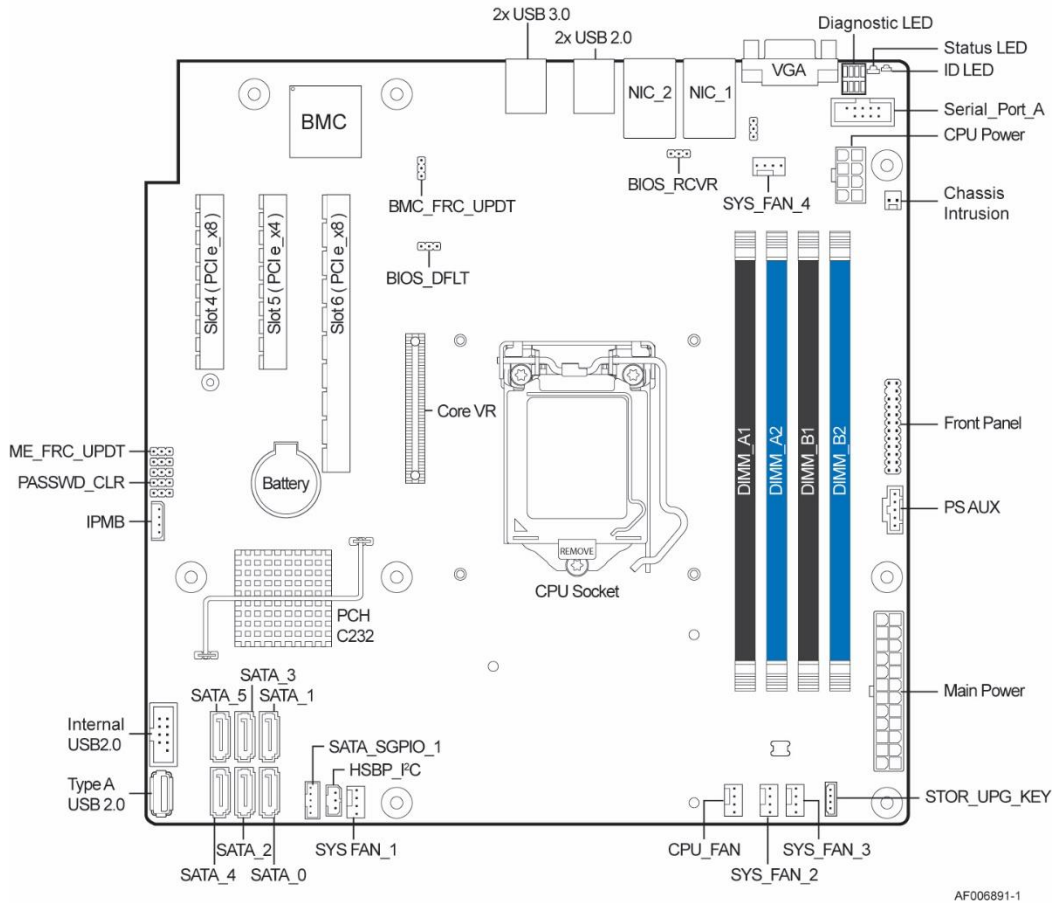
**Figure 3. Intel® Server Board S1200SPS Layout**

## 2.2.2     Server Board Mechanical Drawings
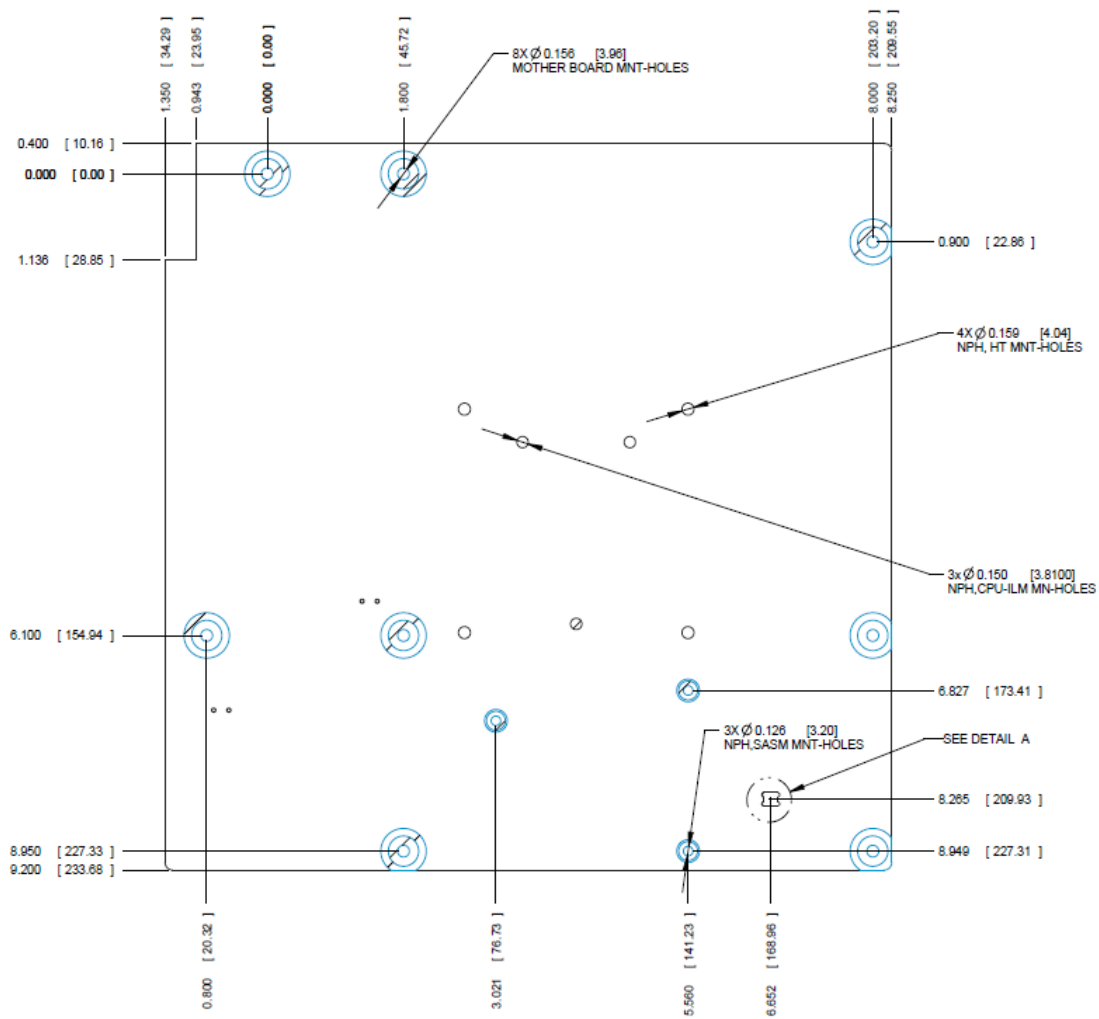


**Figure 4. Intel® Server Board S1200SP – Mounting Hole Locations**
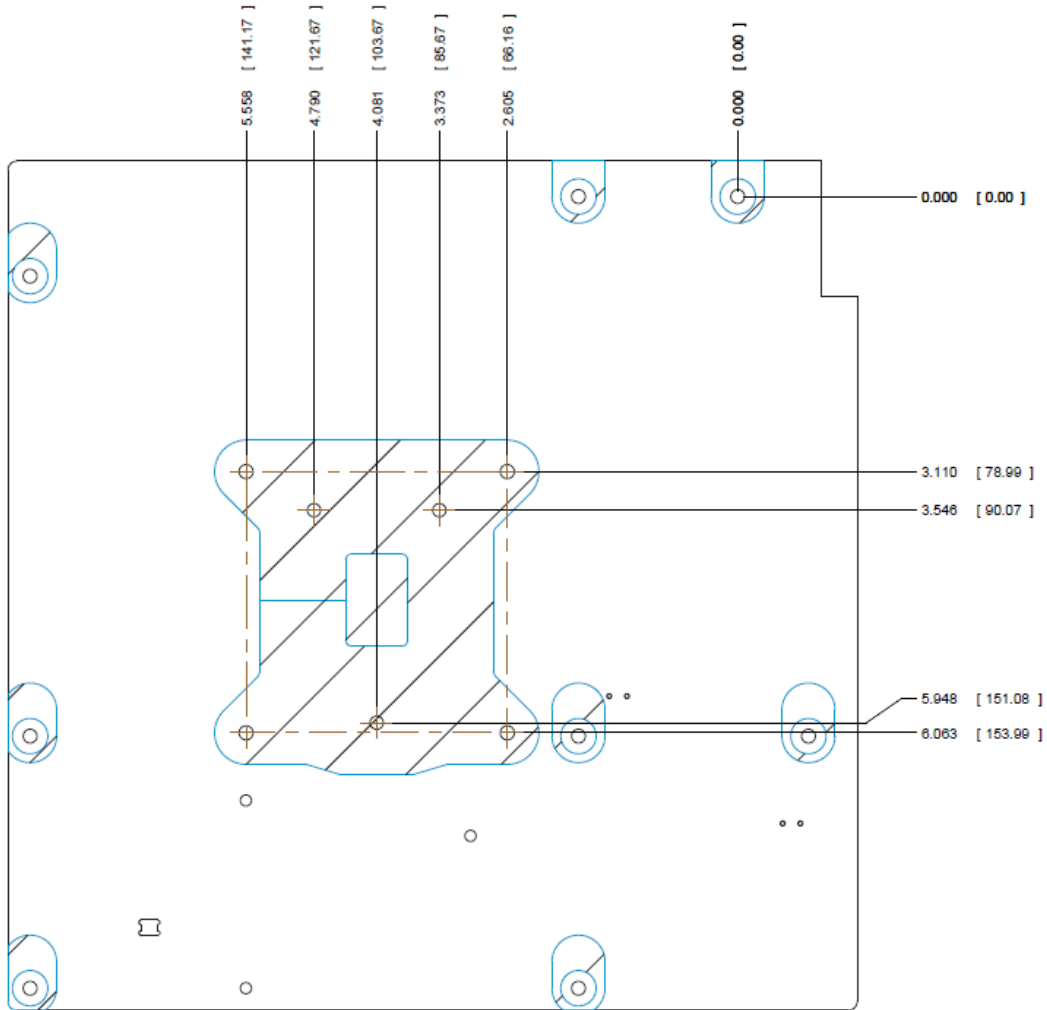
**Figure 5. Intel® Server Board S1200SP – Mounting Hole Locations (continued)**
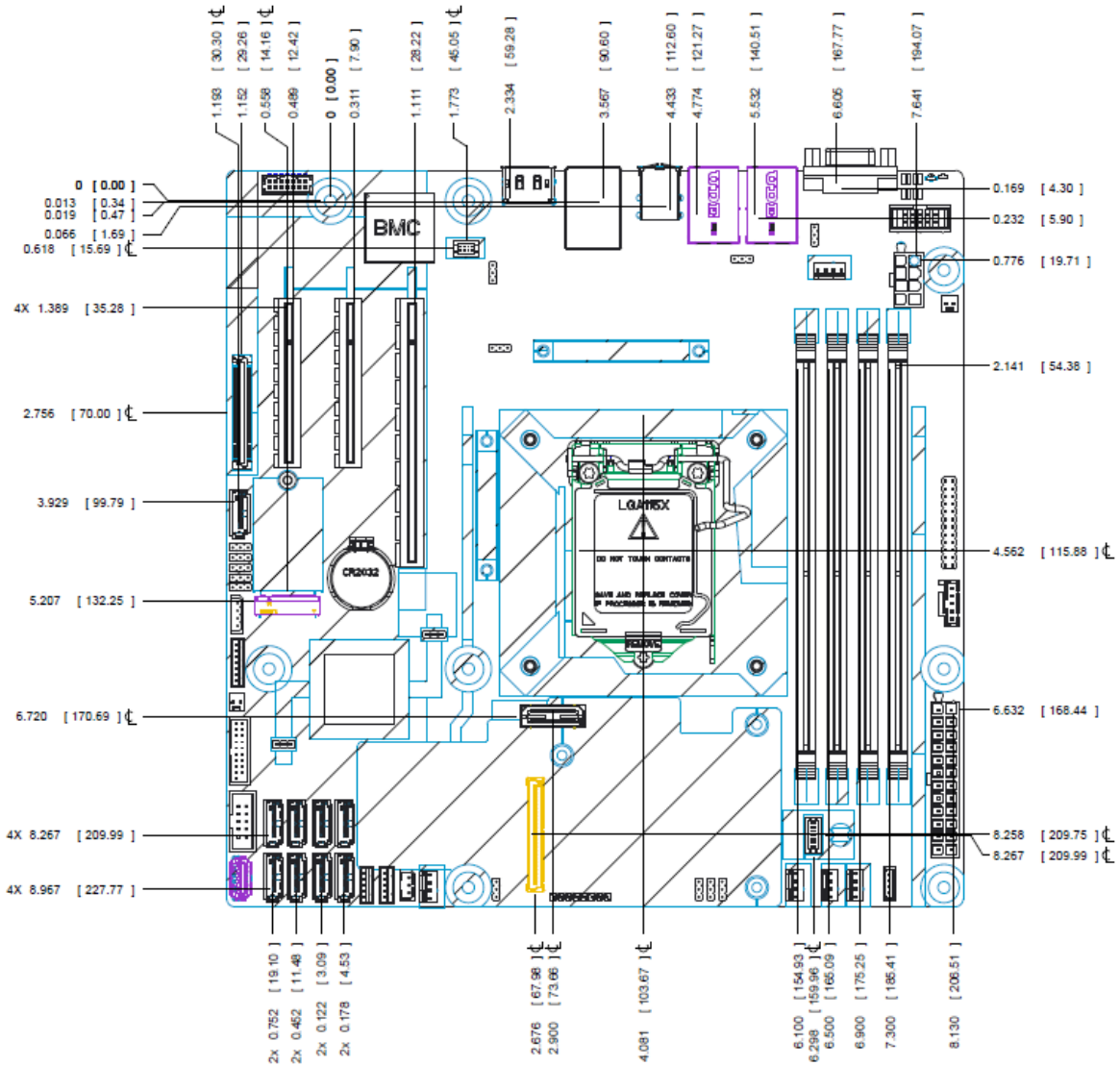
Figure 6. Intel® Server Board S1200SP – Major Connector Pin-1 Locations
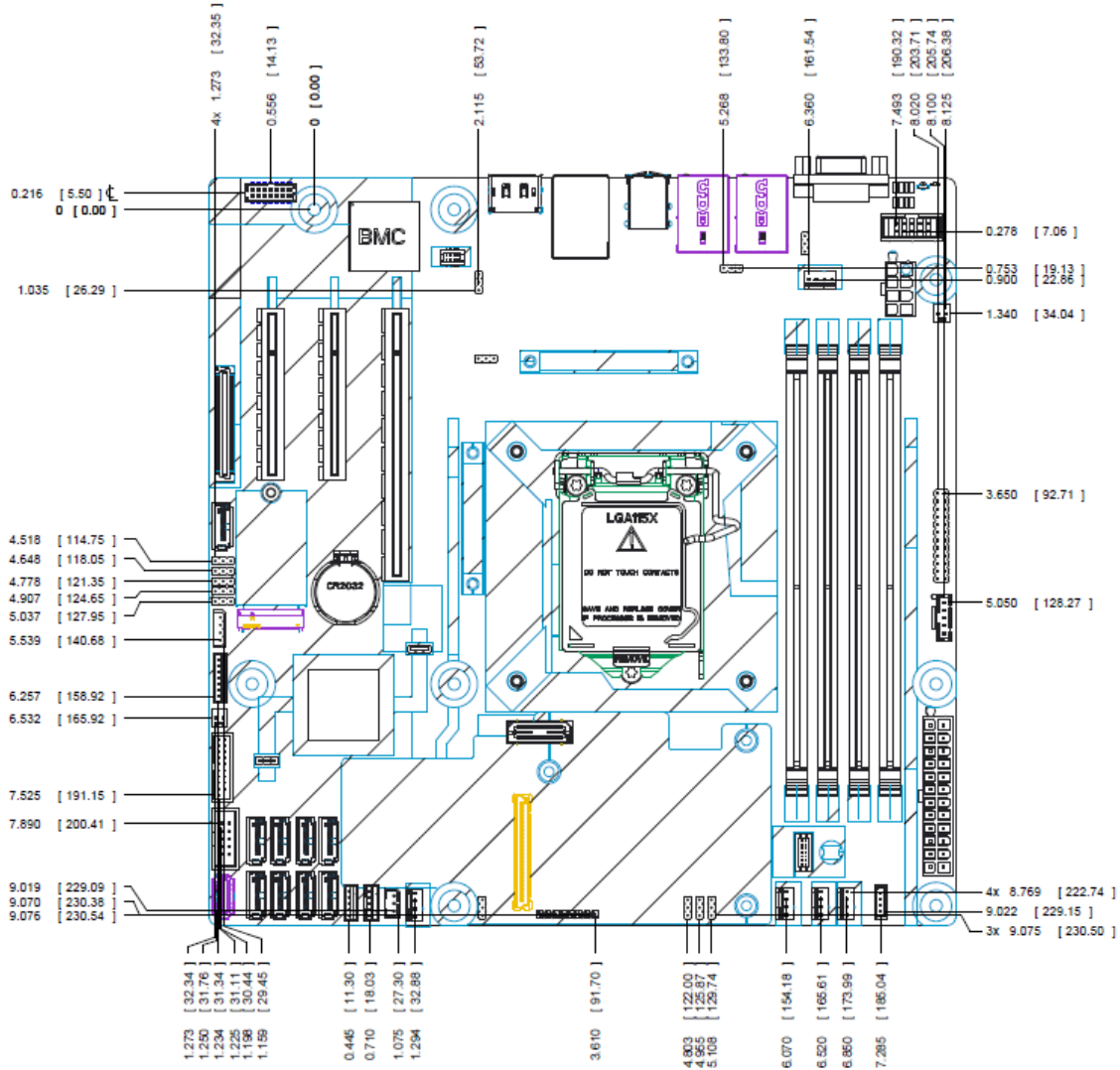
**Figure 7. Intel® Server Board S1200SP – Major Connector Pin-1 Locations (continued)**
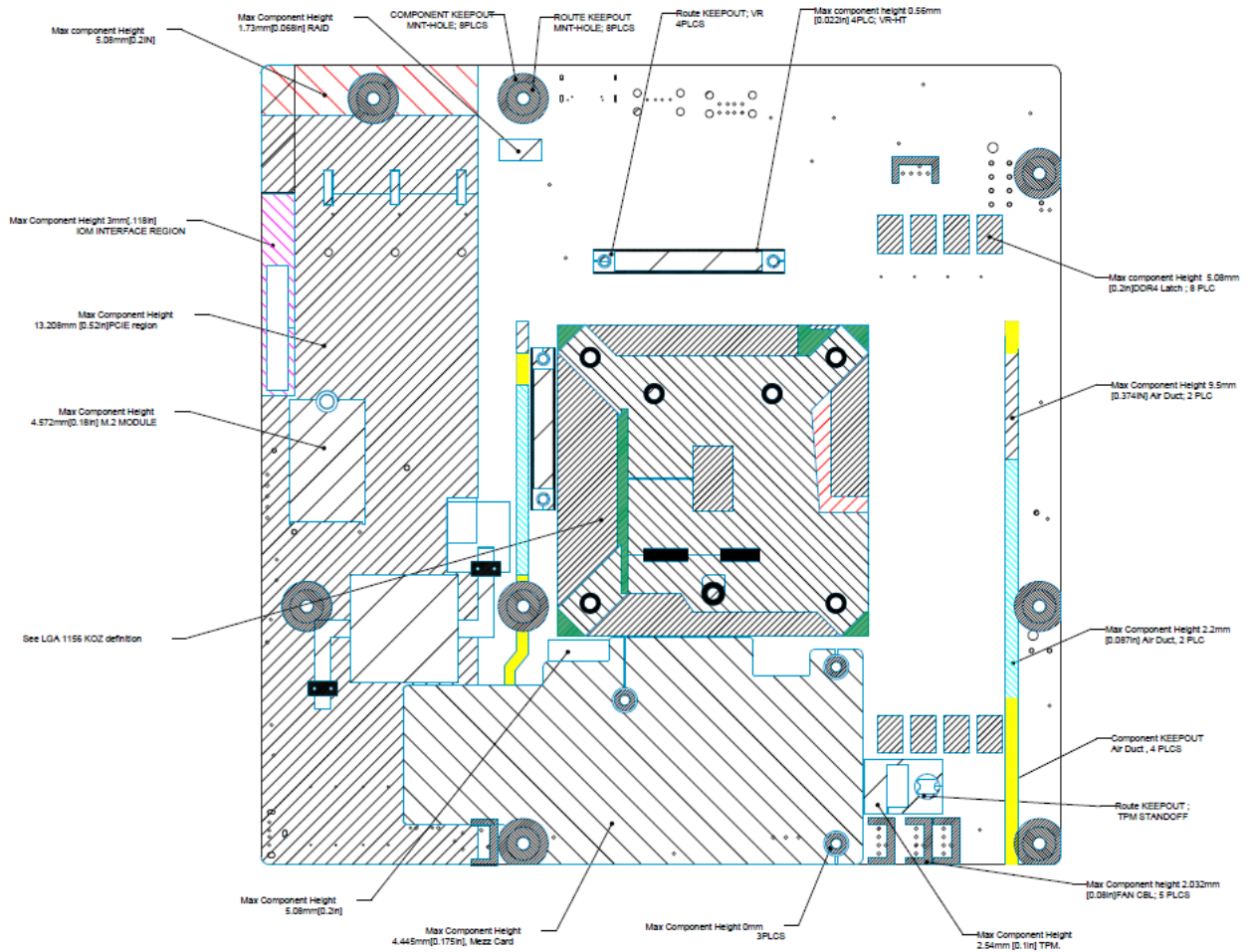
**Figure 8. Intel® Server Board S1200SP – Primary Side Keepout Zone**
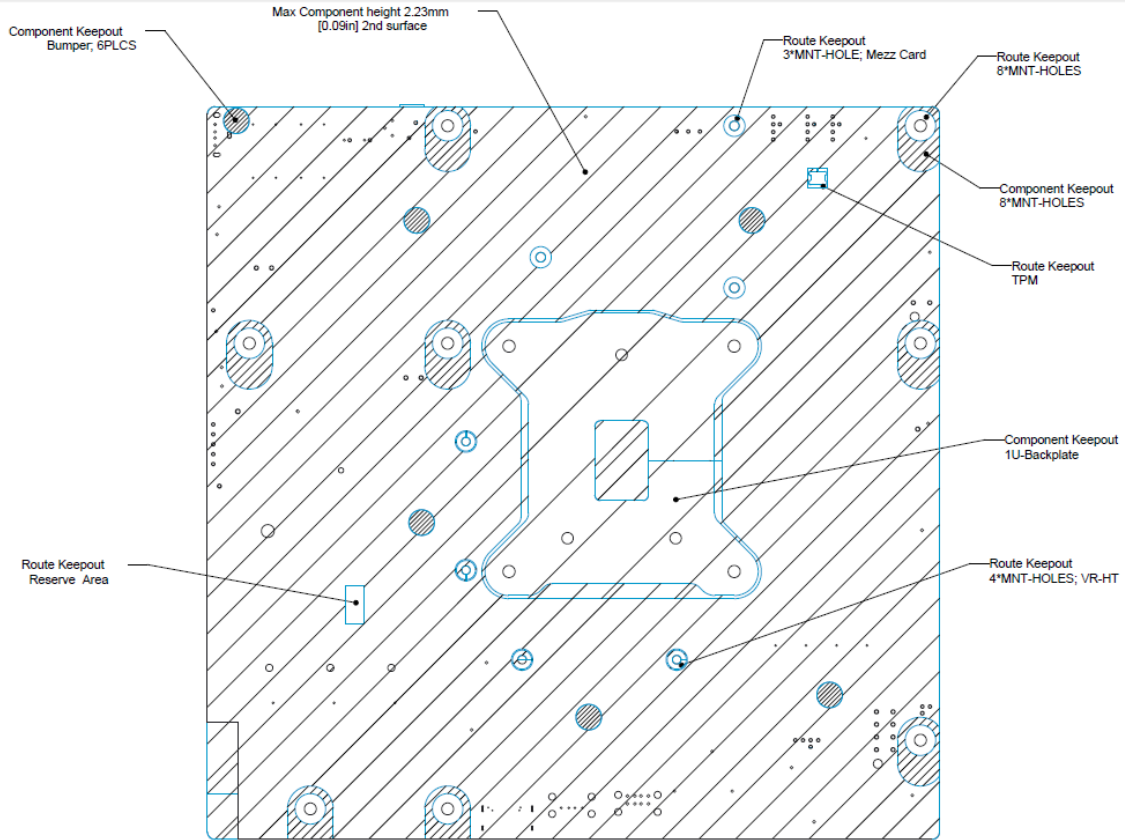
**Figure 9. Intel® Server Board S1200SP – Second Side Keepout Zone**

## 2.2.3     Server Board Rear I/O Layout

The following drawing shows the layout of the rear I/O components for the server boards.
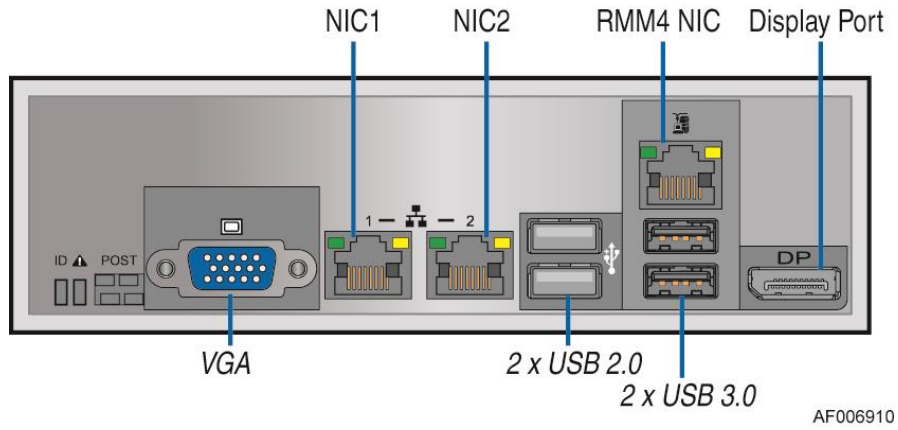


**Figure 10. Intel® Server Board S1200SPL Rear I/O Layout**
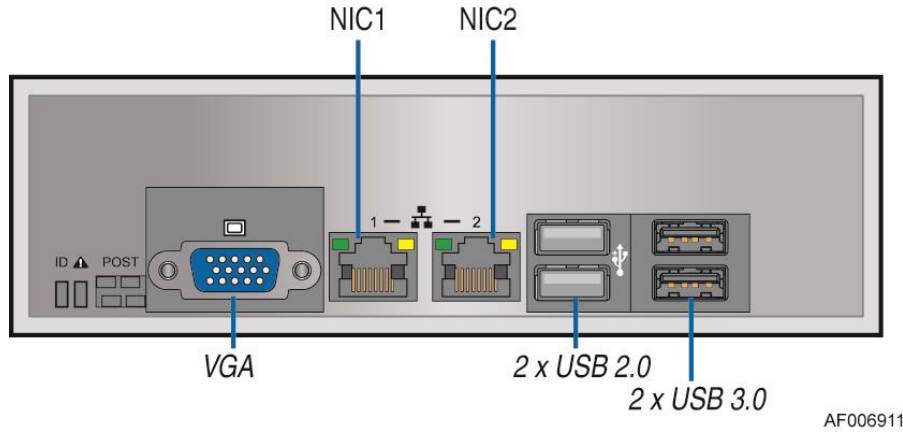


**Figure 11. Intel® Server Board S1200SPS Rear I/O Layout**

# 3.    Functional Architecture

The architecture and design of the Intel® Server Board S1200SP is based on the Intel® C230 series chipset. The chipset is designed for systems based on the Intel® Xeon® processor in an LGA 1151 Socket H4 package.

The Intel® Server Board S1200SPS uses Intel® C232 chipset. The Intel® Server Board S1200SPL uses Intel® C236 chipset.

The Intel® Xeon® Processor E3-1200 V5 Processors are made up of multi-core processors based on the 14nm processor technology. The 6th Intel® Core™ i3 Processors are made up of dual-core processors based on the 14nm processor technology.

This chapter provides a high-level description of the functionality associated with each chipset component and the architectural blocks that make up the server boards.
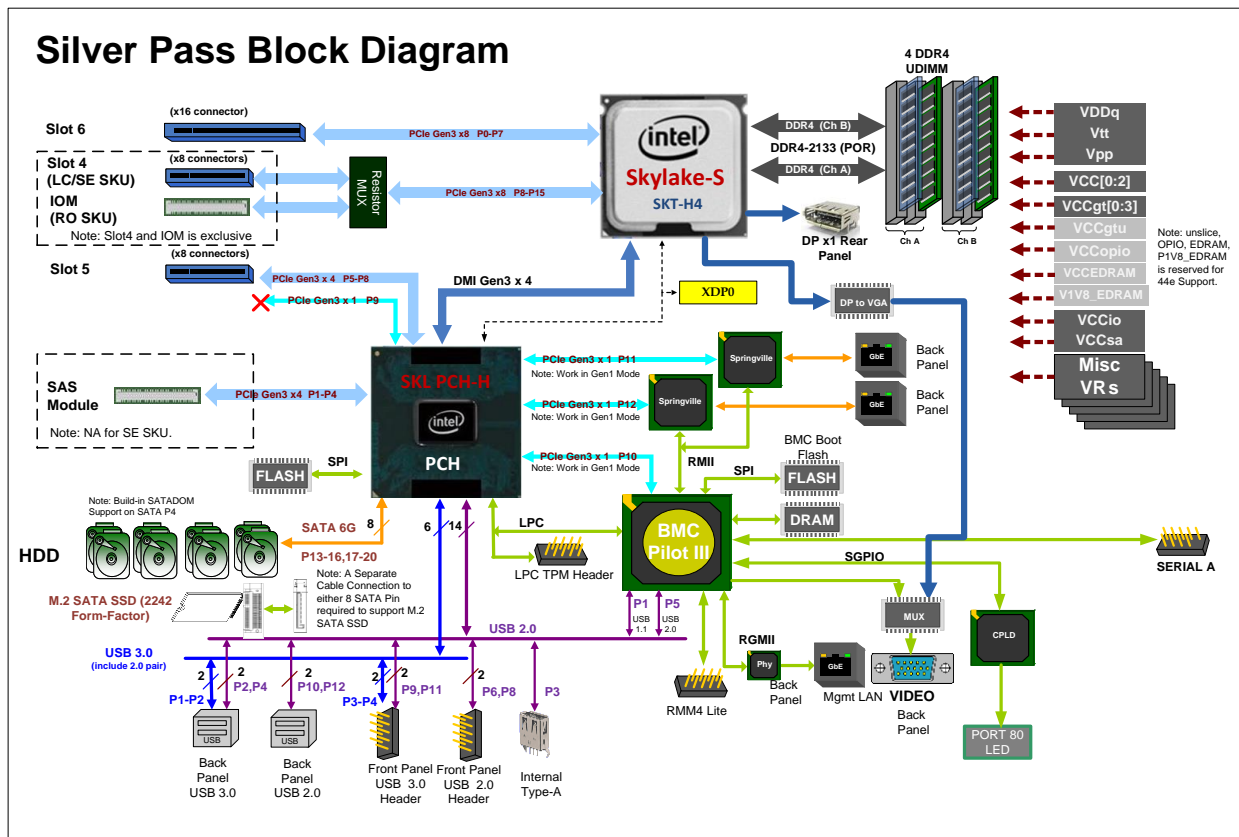


**Figure 12. Intel® Server Board S1200SP Functional Block Diagram**

## 3.1    Processor Subsystem

The Intel® Server Board S1200SP supports the following processor:

- Intel® Xeon® processor E3-1200 V5 product family
- The 6th Generation Intel® Core™ i3 processors

*Note: The previous generation Intel® Xeon® processors are not supported on the Intel® server board described in this document.*

### 3.1.1      Intel® Xeon® processor E3-1200 V5 Product Family

Intel® Xeon® processor E3-1200 v5 product family highly integrated solution variant is composed of quad processor cores:

- LGA 1151 socket package with 8 GT/s
- Up to 80 W Thermal Design Power (TDP)

The list of supported processors may be found at http://serverconfigurator.intel.com/sct_app.aspx.

*Note: The workstation processor is not supported in this platform.*

### 3.1.2      The 6th Generation Intel® Core™ i3 Processors

The 6th Generation Intel® Core™ i3 Processors highly integrated solution variant is composed of Duo cores:

- FC-LGA 1151 socket package with 8 GT/s
- Up to 65 W Thermal Design Power (TDP); processors with higher TDP are not supported

The list of supported processors may be found at http://serverconfigurator.intel.com/sct_app.aspx.

## 3.2    Processor Function Overview

With the release of the Intel® Xeon® processor E3-1200 V5 product family, several key system components, including the CPU, Integrated Memory Controller (IMC), and Integrated IO Module (IIO), have been combined into a single processor package and feature; up to 20 lanes of Gen 3 PCI Express* links.

The following sections provide an overview of the key processor features and functions that help to define the performance and architecture of the server board. For more comprehensive processor specific information, refer to the Intel® Xeon® processor E3-1200 V5 product family documents listed in the Reference Documents list.

Processor feature details:

- Up to four execution cores
- Each core supports two threads (Intel® Hyper-Threading Technology), up to 8 threads per socket

Supported technologies:

- Intel® Virtualization Technology (Intel® VT)
- Intel® Active Management Technology 11.0 (Intel® AMT 11.0)
- Intel® Trusted Execution Technology (Intel® TXT)

- Intel® Streaming SIMD Extensions 4.2 (Intel® SSE4.2)
- Intel® Hyper-Threading Technology (Intel® HT Technology)
- Intel® 64 Architecture
- Execute Disable Bit
- Intel® Turbo Boost Technology 2.0
- Intel® Advanced Vector Extensions 2 (Intel® AVX2)
- Intel® Advanced Encryption Standard New Instructions (Intel® AES-NI)
- PCLMULQDQ (Perform Carry-Less Multiplication Quad word) Instruction
- Intel® Secure Key
- Intel® Transactional Synchronization Extensions (Intel® TSX-NI)
- PAIR – Power Aware Interrupt Routing
- SMEP – Supervisor Mode Execution Protection
- Intel® Boot Guard
- On-package Cache Memory
- Intel® Software Guard Extensions (Intel® SGX)
- Intel® Memory Protection Extensions (Intel® MPX)
- GMM Scoring Accelerator
- Intel® Image Signal Processor (Intel® ISP)
- Intel® Processor Trace

## 3.3 Integrated Memory Controller (IMC) and Memory Subsystem

Integrated into the processor is a memory controller. Only ECC memory is supported on this platform. Each processor provides two DDR4 Unbuffered Dual In-Line Memory Modules (UDIMM) channels that support the following:

- ECC Unbuffered DDR4
- Single-channel and dual-channel memory organization modes
- Data burst length of eight cycles for all memory organization modes
- Memory DDR4 data transfer rates of 1866, and 2133 MT/s
- 64-bit wide channels
- DDR4 I/O Voltage of 1.2 V
- Theoretical maximum memory bandwidth of:
  - 29.8 GB/s in dual-channel mode assuming 1867 MT/s
  - 34.1 GB/s in dual-channel mode assuming 2133 MT/s
- 4 Gb and 8 Gb DDR4 DRAM device technologies are supported
  - Using 4 Gb DRAM device technologies, the largest system memory capacity possible is 32 GB, assuming Dual Channel Mode with four x8 dual ranked DIMM memory configuration
- The memory channels are named as *Channel A* and *Channel B*.

- The memory slots are named as *Slot1* and *Slot2* on each channel. Slot1 is the nearest from the processor socket.

- DIMMs are named to reflect the channel and slot in which they are installed:

  - Channel A, Slot1 is *DIMM_A1*.
  - Channel A, Slot2 is *DIMM_A2*.
  - Channel B, Slot1 is *DIMM_B1*.
  - Channel B, Slot2 is *DIMM_B2*.

## 3.3.1     Supported Memory

- Single Ranked x8 unbuffered ECC
- Dual Ranked x8 unbuffered ECC

**Table 3. UDIMM Support Guidelines**

| Ranks Per DIMM and Data Width | Memory Capacity Per DIMM | | Speed (MT/s) and Voltage Validated by Slot per Channel (SPC) and DIMM Per Channel (DPC) | |
|---|---|---|---|---|
| | | | 2 Slots per Channel | |
| | | | 1DPC | 2DPC |
| | | | 1.2V | 1.2V |
| SRx8 ECC | 4GB | 8GB | 1866, 2133 | 1866 |
| DRx8 ECC | 8GB | 16GB | 1866, 2133 | 1866 |

*Notes:*

1. *No support for RDIMMs.*

2. *No support for SODIMM.*

3. *All channels in a system run at the fastest common frequency.*

4. *Mixing ECC and non-ECC UDIMMs anywhere on the platform is not supported.*

5. *Static CLTT supported using BMC (requires ECC DIMMs with thermal sensor).*

### 3.3.1.1       Memory Population Rules

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

The processor provides two channels of memory, each capable of supporting up to two DIMMs.

- DIMMs are organized into physical slots on DDR4 memory channels that belong to processor socket.

- The silk screened DIMM slot identifiers on the board provide information about the channel. For example, DIMM_A1 is the first slot on Channel A on processor.

- Channel A and Channel B are independent and are not required to have the same number of DIMMs installed. Either channel may be used for a single-DIMM configuration.
  - When only one memory channel is populated, the memory runs in Single Channel mode, with no interleaving.
- When only one memory slot is populated, use the farthest slot in the channel. On Intel® Server Board S1200SP, the farthest slot in the channels are A2 and B2 with blue connectors.

On the Intel® Server Board S1200SP, a total of 4 DIMM slots is provided. The nomenclature for DIMM sockets is detailed in the following table.

**Table 4. Intel® Server Board S1200SP DIMM Nomenclature**

| (0) | | (1) | |
|---|---|---|---|
| Channel A | | Channel B | |
| A1 | A2 | B1 | B2 |
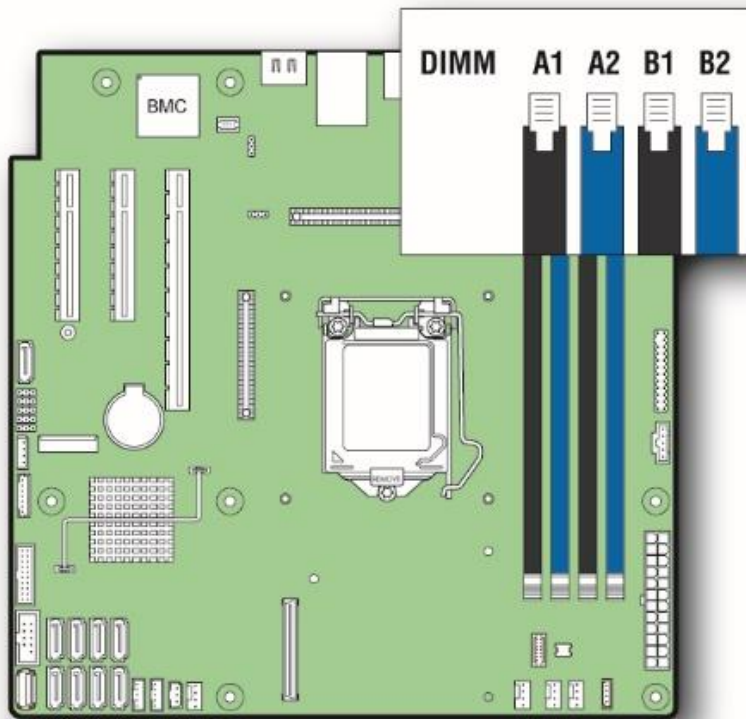


**Figure 13. Intel® Server Board S1200SP DIMM Slot Layout**

**Table 5. Intel® Server Board S1200SP DIMM Maximum Configuration**

| Max Memory Possible | 4Gb DRAM Technology | 8Gb DRAM Technology |
|---|---|---|
| Single Rank UDIMM | 16GB<br>(4 x 4GB DIMMs) | 32GB<br>(4 x 8GB DIMMs) |
| Dual Rank UDIMMs | 32GB<br>(4x 8GB DIMMs) | 64GB<br>(4 x 16GB DIMMs) |

### 3.3.1.2      Publishing System Memory

- The BIOS displays the **Total Memory** of the system during POST if Display Logo is disabled in the BIOS setup. This is the total size of memory discovered by the BIOS during POST, and is the sum of the individual sizes of installed DDR4 DIMMs in the system.

- The BIOS displays the **Effective Memory** of the system in the BIOS setup. The term Effective Memory refers to the total size of all DDR4 DIMMs that are active (not disabled).

- The BIOS provides the total memory of the system in the main page of the BIOS setup. This total is the same as the amount described by the first bullet above.

- If Display Logo is disabled, the BIOS displays the total system memory on the diagnostic screen at the end of POST. This total is the same as the amount described by the first bullet above.

*Note: Some server operating systems do not display the total physical memory installed. What is displayed is the amount of physical memory minus the approximate memory space used by system BIOS components. These BIOS components include, but are not limited to:*

1. *ACPI (may vary depending on the number of PCI devices detected in the system)*

2. *ACPI NVS table*

3. *Processor microcode*

4. *Memory Mapped I/O (MMIO)*

5. *Manageability Engine (ME)*

6. *BIOS flash*

## 3.3.2      Memory RAS Features

For Intel® Server Board S1200SP product family, the form of Memory RAS provided is Error Correction Code (ECC). ECC uses extra bits – 64-bit data in a 72-bit DRAM array – to add an 8-bit calculated Hamming Code to each 64 bits of data. This additional encoding enables the memory controller to detect and report single or double bit errors, and to correct single-bit errors.

There is a specific step in memory initialization in which all of memory is cleared to zeroes before the ECC function is enabled, in order to bring the ECC codes into agreement with memory contents.

During operation, in the process of every fetch from memory, the data and ECC bits are examined for each 64-bit data plus 8-bit ECC group. If the ECC computation indicates that a single bit Correctable Error has occurred, it is corrected and the corrected data is passed on to the processor. If a double-bit Uncorrectable Error is detected, it cannot be corrected. In each case, a Correctable or Uncorrectable ECC Error event is generated.

For Correctable Errors, there is a certain tolerance observed, since a Correctable Error can be generated by something as random as a stray Cosmic Ray impacting the DIMM. Correctable Errors are counted on a per-DIMM basis, but are just silently recorded until the tolerance threshold is crossed. The Correctable Error Threshold for Intel® Server Board S1200SP product family board is set at 10 events. When the 10th CE occurs, a single Correctable Error event is logged.

### 3.3.3 Post Error Codes

The range {0xE0 – 0xEF} of POST codes is used for memory errors in early POST. In late POST, this same range of POST code values is used for reporting other system errors.

- **0xE8 – No Usable Memory Error**: If no usable memory is available, the BIOS emits a beep code and displays POST Diagnostic LED code 0xE8 and halts the system.

  This can also occur if all memory in the system fails and/or has become disabled during memory initialization. For example, if a DDR4 DIMM has no SPD information, the BIOS treats the DIMM slot as if no DDR4 DIMM is present on it. Therefore, if this is the only DDR4 DIMM installed in the system, there is no usable memory, and the BIOS goes to a memory error code 0xE8 as described above.

- **0x53/0x55/0XE8**: DIMM SPD does not respond or DIMM SPD Read Error, the DIMM will not be detected, if the SPD does not respond, which could result in No memory Installed or No Usable Memory Error Halt 0X53, 0x55, or 0xE8, or could result later in an invalid configuration if the no SPD DIMM is in Slot 1 on the channel.

- **0x51 – Memory SPD Error**: If the DIMM does respond but the SPD cannot be successfully read, that would cause a Memory SPD Error, memory error halt 0X51. For each memory channel, once the DIMM SPD parameters have been read, they are checked to verify that the DIMMs on the channel are a valid configuration, DIMM speed and size, ECC capability, and in which memory slot the DIMMs are installed. An invalid configuration will cause the system to halt.

- **0xEA – Channel Training Error**: If the memory initialization process is unable to properly perform the Data/Data Strobe timing training on a memory channel, the BIOS emits a beep code and displays POST Diagnostic LED code 0xEA momentarily during the beeping. If there is usable memory in the system on the other channel, POST memory initialization continues. Otherwise, the system beeps and halts with POST Diagnostic LED code 0xEA staying displayed.

- **0x54/0xEB – Memory Test Error**: If a DDR4 DIMM or a set of DDR4 DIMMs on the same memory channel fails memory testing but usable memory remains available, the BIOS emits a beep code and displays POST Diagnostic LED code 0xEB momentarily during the beeping, then continues POST. If all of the memory fails memory testing, then system memory error code 0xE8 (No Usable Memory) as described above.

- **0xED – Population Error or Invalid DIMM**: If the installed memory contains an invalid DIMM configuration on either channel in the system, the system beeps and halts with POST Diagnostic LED code 0xED. The DIMM are installed incorrectly, not following the *Fill Farthest First* rule (Slot 1 must be filled before Slot 2). This will result in a DIMM Population Error, with a Memory Error Halt 0xED.

### 3.3.4 Processor Integrated I/O Module (IIO)

The processor's integrated I/O module provides features traditionally supported through chipset components. The integrated I/O module provides the following features:

- **PCI Express* Interfaces**

The integrated I/O module incorporates the PCI Express* interface and supports up to 16 lanes of PCI Express*. Following are key attributes of the PCI Express* interface:

- Gen3 speeds at 8 GT/s (no 8b/10b encoding)
- Can operate at 2.5 GT/s, 5 GT/s, or 8 GT/s

The Intel® Server Board S1200SP support PCIe* slots:

- Slot 6: PCI Express* Gen3 x8 electrical with x16 physical connector, from processor.
- Slot 5: PCI Express* Gen3 x4 electrical with x8 physical connector, from PCH.
- Slot 4: PCI Express* Gen3 x8 electrical with x8 physical connector, from processor.

▪ **Direct Media Interface (DMI)**

Direct Media Interface (DMI) connects the processor and the PCH. DMI2.0 is supported.

*Note: Only DMI Gen3 x4 configuration is supported.*

- DMI 2.0 support
- Compliant to Direct Media Interface Second Generation (DMI2).
- Four lanes in each direction.
- 8 GT/s point-to-point DMI interface to PCH is supported.

## 3.3.5    Intel® Integrated RAID Option

The Intel® Server Board S1200SPL provides a SAS/ROC Mezzanine slot (J4J1) to a high density 80-pin connector labeled *SAS_MOD* for the installation of an optional Intel® Integrated RAID Module.

Features of this option include:

▪ SKU options to support full or entry level hardware RAID

▪ Dual-core 6Gb SAS/SATA ROC/IOC (LSI* 2208 and 2308)

▪ 12Gb SAS ROC/IOC (LSI* 3008 and 3108)

▪ 4 or 8 ports and SAS/SATA or SATA

▪ SKU options to support 512MB or 1GB embedded memory

▪ Intel® designed flash plus optional support for Intel® RAID Maintenance Free Backup Units (AXXRMFBU2/AXXRMFBU5) or Intel® RAID Smart Battery AXXRSBBU9.

For supported SAS modules, refer to the document *Intel® Server Boards S1200SP Configuration Guide and Spares/Accessories List*

For additional product information, refer to the document *Intel® Integrated RAID Module RMS25KB080, RMS25KB040, RMS25CB080, and RMS25CB040 Hardware User's Guide*.

## 3.3.6    Intel® I/O Acceleration Technolgy 2 (Intel® I/O AT2)

Intel® I/O AT2 is not supported.

### 3.3.6.1      Direct Cache Access (DCA)

Direct Cache Access (DCA) is not supported on Intel® Xeon® Processor E3-1200 v5 series.

## 3.4   Intel® C230 Series Chipset PCH Functional Overview

The following subsections provide an overview of the key features and functions of the Intel® C230 series chipset PCH used on the server board. For more comprehensive chipset specific information, refer to the Intel® C230 series chipset documents listed in the [Reference Document](#) list.

**Table 6. Intel® C230 Series Chipset Features**

|  | C232 | C236 |
|---|---|---|
| Flex I/O Support | Yes | Yes |
| Total SATA 3.0 Ports | 6 | Up to 8 |
| Total PCIe* Lanes | 8 | UP to 20 |
| Total USB 3.0 Ports | 6 | Up to 10 |
| Total USB 2.0 Ports | 12 | 14 |
| ME FW | SPS | SPS and ME11 |
| SATA Express Capable Port | No | Up to 3 |
| CPU pGFX | No | Yes |

On the Intel® Server Boards S1200SP, the chipset provides support for the following on-board functions:

- Digital Media Interface (DMI) to Processor
- PCI Express* Interface
- Serial ATA (SATA) Controller
- AHCI
- Rapid Storage Technology enterprise (RSTe)
- Low Pin Count (LPC) interface
- Serial Peripheral Interface (SPI)
- Compatibility Modules (DMA Controller, Timer/Counters, Interrupt Controller)
- Advanced Programmable Interrupt Controller (APIC)
- Universal Serial Bus (USB) Controller
- Gigabit Ethernet Controller
- RTC
- GPIO
- Enhanced Power Management
- Manageability
- System Management Bus (SMBus* 2.0)
- Integrated NVSRAM controller
- Virtualization Technology for Direct I/O (Intel® VT-d)
- JTAG Boundary-Scan
- KVM/Serial Over LAN (SOL) Function

### 3.4.1 Digital Media Interface (DMI)

Digital Media Interface (DMI) is the chip-to-chip connection between the processor and the Intel® C230 series chipset. This high-speed interface integrates advanced priority-based servicing allowing for concurrent traffic and true isochronous transfer capabilities. Base functionality is completely software-transparent, permitting current and legacy software to operate normally.

### 3.4.2 PCI Express* Interface

The Intel® C230 series chipset provides up to 20 PCI Express* Root Ports, supporting the PCI Express* Base Specification, Revision 3.0. Each Root Port x1 lane supports up to 8 Gb/s bandwidth in each direction (16 Gb/s concurrent). On the Intel® Server Board S1200SPL, PCI Express* Root Ports 1-4 are configured to support one Gen3 x4 port widths of SAS Module connector; on the Intel® Server Board S1200SPL and S1200SPS, PCI Express* Root Ports 5-8 are configured to support one Gen3 x4 port widths of slot 5. On the Intel® Server Boards S1200SP family product, PCI Express* Root Port 10 is configured to support one Gen1 x1 widths connection with the BMC chip; PCI Express* Root Port 11 and 12 are configured to support two Gen1 x1 widths connection with the two Intel® I210 Gigabit Ethernet Network controller.

### 3.4.3 Serial ATA (SATA) Controller

The Intel® C230 series chipset provides:

- SATA host controllers that support independent DMA operation on up to eight ports and supports data transfer rates of up to 6.0 Gb/s (600 MB/s). The SATA controller contains two modes of operation – a legacy mode using I/O space, and an AHCI mode using memory space. Software that uses legacy mode will not have AHCI capabilities. The Intel® C230 series chipset supports the Serial ATA Specification, Revision 3.0. The Intel® C230 series also supports several optional sections of the Serial ATA II: Extensions to Serial ATA 1.0 Specification, Revision 1.0 (AHCI support is required for some elements).

- One M.2 SATA SSD 2242 Module with a separate SATA cable to any of the on-board SATA Connector

- Two 5-pin SATA SGPIO connectors, one to cover drive 0-3 with SDATAOUT0, the other to cover drive 4-7 with SDATAOUT1

- SATADOM with native power from SATA connector directly on port 4 (cable-less)

- AHCI

The Intel® C230 series chipset provides hardware support for Advanced Host Controller Interface (AHCI), a standardized programming interface for SATA host controllers. Platforms supporting AHCI may take advantage of performance features such as no master/slave designation for SATA devices—each device is treated as a master—and hardware assisted native command queuing. AHCI also provides usability enhancements such as Hot-Plug. AHCI requires appropriate software support (for example, an AHCI driver) and for some features, hardware support in the SATA device or additional platform hardware.

The server board includes support for two embedded software RAID options:

- Intel® Embedded Server RAID Technology 2 (ESRT2) based on LSI* MegaRAID SW RAID technology

- Intel® Rapid Storage Technology (RSTe)

Using the <F2> BIOS Setup Utility, accessed during system POST, options are available to enable/disable SW RAID, and select which embedded software RAID option to use.

### 3.4.3.1        Intel® Rapid Storage Technology Enterprise

The Intel® C230 series chipset provides support for Intel® Rapid Storage Technology enterprise, providing both AHCI (see above for details on AHCI) and integrated RAID functionality. The industry-leading RAID capability provides high-performance RAID 0, 1, 5, and 10 functionality on up to 8 SATA ports of the Intel® C230 series chipset. RSTe RAID support is provided to allow multiple RAID levels to be combined on a single set of hard drives, such as RAID 0 and RAID 1 on two disks. Other RAID features include hot-spare support, SMART alerting, and RAID 0 auto replace. Software components include an Option ROM for pre-boot configuration and boot functionality, a Microsoft Windows* compatible driver, and a user interface for configuration and management of the RAID capability of the Intel® C230 series chipset.

### 3.4.3.2        Intel® Embedded Server RAID Technology 2 (ESRT2)

Features of the embedded software RAID option Intel® Embedded Server RAID Technology 2 (ESRT2) include the following:

- Based on LSI* MegaRAID Software Stack
- Software RAID with system providing memory and CPU utilization
- Supported RAID Levels – 0, 1, 10
- RAID 5 support provides with upgrade key of RKSATA8R5. RAID 5 under legacy BIOS mode is not supported.
- Open Source Compliance = Binary Driver (includes Partial Source files) or Open Source using MDRAID layer in Linux*
- OS Support = Microsoft Windows 2012*, Microsoft Windows 2008*, RHEL*, SLES, and other Linux* variants using partial source builds
- Utilities = Microsoft Windows* GUI and CLI, Linux* GUI and CLI, DOS CLI, and EFI CLI

## 3.4.4        Low Pin Count (LPC) Interface

The Intel® C230 series chipset implements an LPC Interface as described in the *LPC 1.1 Specification* and provides support for up to two Master/DMI devices. On the server board, the LPC interface is utilized as an interconnection between the chipset and the Integrated Base Board Management Controller as well as providing support for the optional Trusted Platform Module (TPM).

## 3.4.5        Serial Peripheral Interface (SPI)

The Intel® C230 series chipset implements an SPI Interface as an alternative interface for the BIOS flash device.

## 3.4.6        Universal Serial Bus (USB) Controller

The Intel® C230 series chipset contains an eXtensible Host Controller Interface (xHCI) host controller which supports up to fourteen USB 2.0 ports and up to six USB 3.0 ports. This controller allows data transfers of up to 5Gb/s. The controller supports SuperSpeed (SS), high-speed (HS), full-speed (FS), and low speed (LS) traffic on the bus.
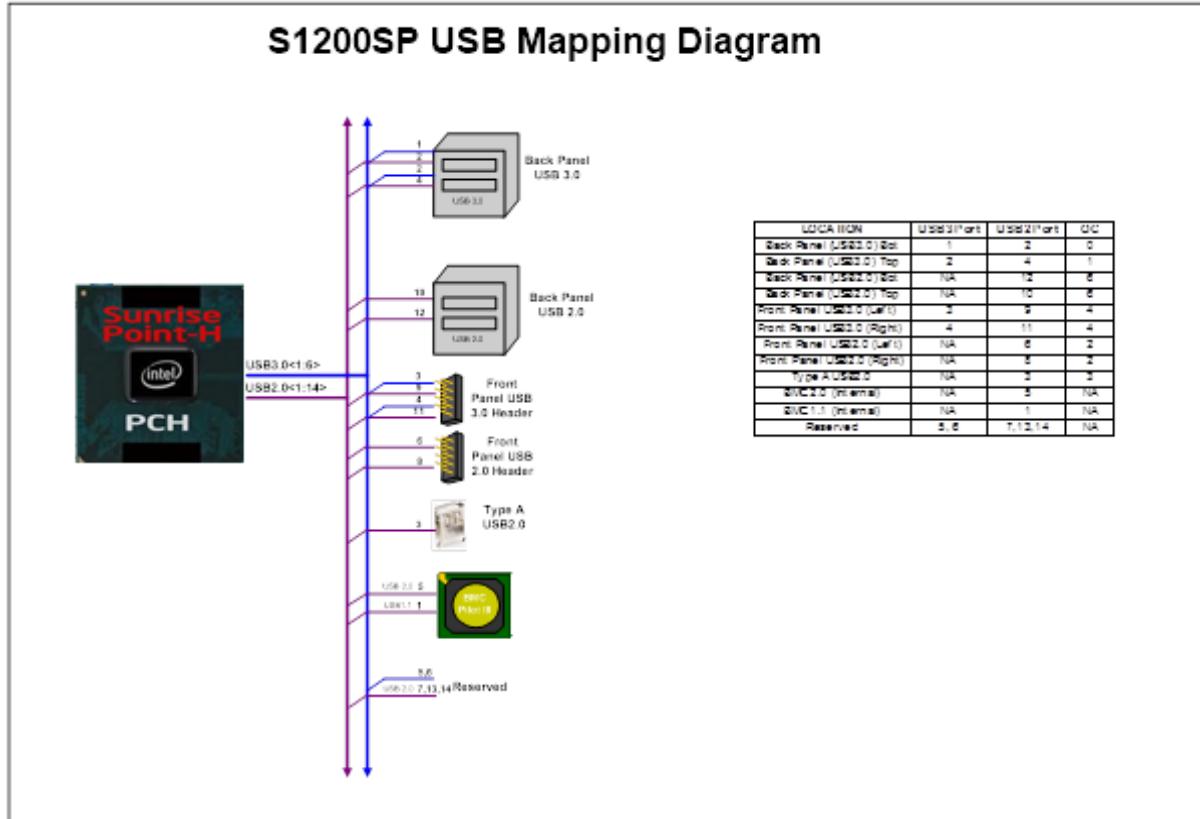
**Figure 14. Intel® Server Board S1200SP Series USB Mapping Diagram**

### 3.4.6.1         Native USB Support

During the power-on self-test (POST), the BIOS initializes and configures the USB subsystem. The BIOS can initialize and use the following types of USB devices:

- USB Specification-compliant keyboards
- USB Specification-compliant mouse
- USB Specification-compliant storage devices that utilize bulk-only transport mechanism

USB devices are scanned to determine if they are required for booting.

The BIOS supports USB 2.0 mode of operation, and as such supports USB 1.1 and USB 2.0 compliant devices and host controllers.

During the pre-boot phase, the BIOS automatically supports the hot addition and hot removal of USB devices and a short beep is emitted to indicate such an action. For example, if a USB device is hot plugged, the BIOS detects the device insertion, initializes the device, and makes it available to the user. During POST, when the USB controller is initialized, it emits a short beep for each USB device in the system as if they were all just "hot added".

Only on-board USB controllers are initialized by BIOS. This does not prevent the operating system from supporting any available USB controllers including add-in cards.

### 3.4.6.2         Legacy USB Support

The BIOS supports PS/2 emulation of USB keyboards and mouse. During POST, the BIOS initializes and configures the root hub ports and searches for a keyboard and/or a mouse on the USB hub and then enables the devices that are recognized.

## 3.4.7         Gigabit Ethernet Controller
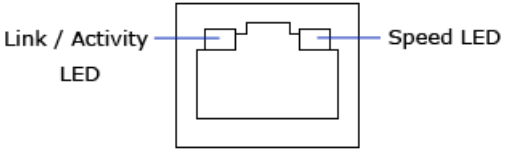
Network connectivity is provided by means of two onboard Intel® Ethernet Controller I210 providing up to two 10/100/1000 Mb Ethernet ports. The Intel® Ethernet Controller I210 is single, compact, low-power components that offer a fully-integrated Gigabit Ethernet Media Access Control (MAC) and Physical Layer (PHY) port. The Intel® Ethernet Controller I210 uses the PCI Express* architecture from the Intel® C230 series PCH and provides a single-port implementation in a relatively small area so it can be used for server and client configurations as a LAN on Motherboard (LOM) design.

External interfaces provided on the I210:

- ▪ PCIe Rev. 2.0 (2.5 GHz) x1
- ▪ MDI (Copper) standard IEEE 802.3 Ethernet interface for 1000BASE-T, 100BASETX, and 10BASE-T applications (802.3, 802.3u, and 802.3ab)
- ▪ NC-SI or SMBus* connection to a Manageability Controller (MC)
- ▪ EEE 1149.1 JTAG (note that BSDL testing is NOT supported)

Each Ethernet port drives two LEDs located on each network interface connector. The LED at the right of the connector is the link/activity LED and indicates network connection when on, and transmit/receive activity when blinking. The LED at the left of the connector indicates link speed as defined in the following table.

**Table 7. External RJ45 NIC Port LED Definition**



| LED Color | LED State | NIC State |
|---|---|---|
| Green/Amber (Right) | Off | 10 Mbps |
|  | Amber | 100 Mbps |
|  | Green | 1000 Mbps |
| Green (Left) | On | Active Connection |
|  | Blinking | Transmit/Receive activity |

### 3.4.7.1         MAC Address Definition

Intel® Server Board S1200SPL has the following MAC addresses assigned to them at the factory:

- ▪ NIC 1 MAC address (for OS usage)
- ▪ NIC 2 MAC address = NIC 1 MAC address + 1 (for OS usage)
- ▪ BMC LAN channel 1 MAC address = NIC1 MAC address + 2

- BMC LAN channel 2 MAC address = NIC1 MAC address + 3
- BMC LAN channel 3 (DMN) MAC address = NIC1 MAC address + 4

Intel® Server Board S1200SPS has the following MAC addresses assigned to it at the factory:

- NIC 1 MAC address (for OS usage)
- NIC 2 MAC address = NIC 1 MAC address + 1 (for OS usage)
- BMC LAN channel 1 MAC address = NIC1 MAC address + 2
- BMC LAN channel 2 MAC address = NIC1 MAC address + 3

## 3.4.8 Serial Ports

The server board provides a nine-pin internal DH-10 serial header. You can use a standard DH-10 to DB9 cable to direct serial A port to the rear of a chassis.

## 3.4.9 KVM/Serial Over LAN (SOL) Function

These functions support redirection of keyboard, mouse, and text screen to a terminal window on a remote console. The keyboard, mouse, and text redirection enables the control of the client machine through the network without the need to be physically near that machine. Text, mouse, and keyboard redirection allows the remote machine to control and configure the client by entering BIOS setup. The KVM/SOL function emulates a standard PCI serial port and redirects the data from the serial port to the management console using LAN. KVM has additional requirements of internal graphics and SOL may be used when KVM is not supported.

## 3.4.10 System Management Bus (SMBus* 2.0)

The Intel® C230 series chipset contains a SMBus* Host interface that allows the processor to communicate with SMBus* slaves. This interface is compatible with most I²C devices. Special I²C commands are implemented. The Intel® C230 series chipset's SMBus* host controller provides a mechanism for the processor to initiate communications with SMBus* peripherals (slaves). Also, the Intel® C230 series chipset supports slave functionality, including the Host Notify protocol. Hence, the host controller supports eight command protocols of the SMBus* interface (see *System Management Bus (SMBus*) Specification, Version 2.0*): Quick Command, Send Byte, Receive Byte, Write Byte/Word, Read Byte/Word, Process Call, Block Read/Write, and Host Notify.

The Intel® C230 series chipset's SMBus* also implements hardware-based Packet Error Checking for data robustness and the Address Resolution Protocol (ARP) to dynamically provide address to all SMBus* devices.

## 3.4.11 Intel® Virtualization Technology for Direct I/O (Intel® VT-d)

The Intel® C230 series chipset provides hardware support for implementation of Intel® Virtualization Technology with Directed I/O (Intel® VT-d). Intel® VT-d Technology consists of technology components that support the virtualization of platforms based on Intel® Architecture Processors. Intel® VT-d Technology enables multiple operating systems and applications to run in independent partitions. A partition behaves like a Virtual Machine (VM) and provides isolation and protection across partitions. Each partition is allocated its own subset of host physical memory.

## 3.5    Integrated Baseboard Management Controller (BMC) Overview

The Integrated BMC is provided by an embedded ARM9* controller and associated peripheral functionality that is required for IPMI-based server management. Firmware usage of these hardware features is platform dependent.

The following is a summary of the Integrated BMC management hardware features that comprise the BMC:

- IPMI 2.0 Compliant
- 400MHz 32-bit ARM9* processor with memory management unit (MMU)
- Two independent 10/100/1000 Mb/s Ethernet Controllers with RMII/RGMII support
- DDR2/3 16-bit interface with up to 800 MHz operation
- Sixteen 10-bit ADCs
- Sixteen fan tachometers
- Eight Pulse Width Modulators (PWM)
- Chassis intrusion logic
- JTAG Master
- Eight I$^2$C interfaces with master-slave and SMBus* timeout support. All interfaces are SMBus* 2.0 compliant.
- Parallel general-purpose I/O Ports (16 direct, 32 shared)
- Serial general-purpose I/O Ports (80 in and 80 out)
- Three UARTs
- Platform Environmental Control Interface (PECI)
- Six general-purpose timers
- Interrupt controller
- Multiple Serial Peripheral Interface (SPI) flash interfaces
- NAND/Memory interface
- Sixteen mailbox registers for communication between the BMC and host
- LPC ROM interface
- BMC watchdog timer capability
- SD/MMC card controller with DMA support
- LED support with programmable blink rate controls on GPIOs
- Port 80h snooping capability
- Secondary Service Processor (SSP), which provides the HW capability of offloading time critical processing tasks from the main ARM* core.
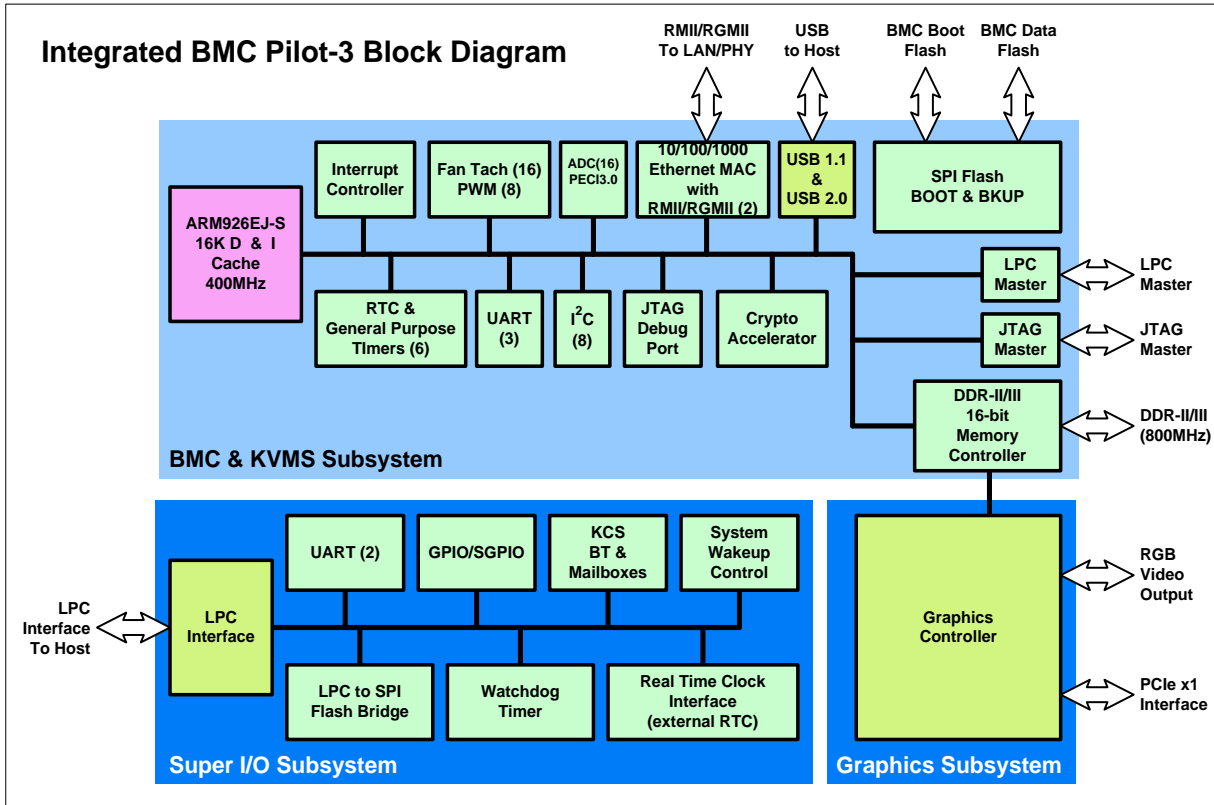
**Figure 15. Integrated BMC Functional Block Diagram**

Emulex* Pilot III contains an integrated SIO, KVMS subsystem and graphics controller with the following features:

### 3.5.1    Super I/O Controller

The integrated super I/O controller provides support for the following features as implemented on the server board:

- Keyboard Style/BT interface for BMC support
- Two Fully Functional Serial Ports, compatible with the 16C550
- Serial IRQ Support
- Up to 16 Shared GPIO available for host processor
- Programmable Wake-up Event Support
- Plug and Play Register Set
- Power Supply Control

### 3.5.2    Remote Keyboard, Video, Mouse, and Storage (KVMS)

The Integrated BMC contains a remote KVMS subsystem with the following features:

- USB 2.0 interface for Keyboard, Mouse and Remote storage such as CD/DVD ROM and floppy
- USB 1.1/USB 2.0 interface for PS2 to USB bridging, remote Keyboard and Mouse

- Hardware Based Video Compression and Redirection Logic
- Supports both text and Graphics redirection
- Hardware assisted Video redirection using the Frame Processing Engine
- Direct interface to the Integrated Graphics Controller registers and Frame buffer
- Hardware-based encryption engine

### 3.5.2.1 Integrated BMC Embedded LAN Channel

The Integrated BMC hardware includes two dedicated 10/100 Mb/s network interfaces. These interfaces are not shared with the host system. At any time, only one dedicated interface may be enabled for management traffic. The default active interface is the NIC 1 port.

For these channels, support can be enabled for IPMI-over-LAN and DHCP. For security reasons, embedded LAN channels have the following default settings:

- IP Address: Static
- All users disabled

## 3.5.3 Graphics Controller and Video Support

The integrated graphics controller provides support for the following features as implemented on the server board:

- Integrated Graphics Core with 2D Hardware accelerator
- DDR-3 memory interface supporting up to 128MB of memory, 16MB allocated to graphic
- Supports display resolutions up to 1920 x 1200 16bpp @ 60Hz
- High speed Integrated 24-bit RAMDAC
- Single lane PCI Express* host interface running at Gen 1 speed

The integrated video controller supports all standard IBM VGA modes. The following table shows the 2D modes supported for both CRT and LCD.

**Table 8. Onboard Video Resolution and Refresh Rate (Hz)**

| 2D Mode | 2D Video Mode Support (Color Bit) | | | |
|---------|--------|---------|---------|---------|
| Resolution | 8 bpp | 16 bpp | 24 bpp | 32 bpp |
| 640x480 | 60, 72, 75, 85 | 60, 72, 75, 85 | Not supported | 60, 72, 75, 85 |
| 800x600 | 60, 72, 75, 85 | 60, 72, 75, 85 | Not supported | 60, 72, 75, 85 |
| 1024x768 | 60, 70, 75, 85 | 60, 70, 75, 85 | Not supported | 60, 70, 75, 85 |
| 1152x864 | 75 | 75 | 75 | 75 |
| 1280x800 | 60 | 60 | 60 | 60 |
| 1280x1024 | 60 | 60 | 60 | 60 |
| 1440x900 | 60 | 60 | 60 | 60 |
| 1600x1200 | 60 | 60 | Not Supported | Not Supported |
| 1680x1050 | 60 | 60 | Not Supported | Not Supported |

| 2D Mode | 2D Video Mode Support (Color Bit) | | | |
|---|---|---|---|---|
| Resolution | 8 bpp | 16 bpp | 24 bpp | 32 bpp |
| 1920x1080 | 60 | 60 | Not Supported | Not Supported |
| 1920x1200 | 60 | 60 | Not Supported | Not Supported |

*Note: Video resolutions at 1600x1200 and higher are only supported through the external video connector located on the rear I/O section of the server board.*

On Intel® Server Board S1200SPL, the display port is supported from the processor. A display port to VGA convertor and a VGA mux are implemented to enable VGA output from processor graphics. Users can set "Primary Display" option in BIOS to Add-in Graphics or VGA Port or Display Port and set "VGA Port Output" option to Onboard Video or Processor Graphics.

# 4.    System Security

## 4.1    BIOS Password Protection

The BIOS uses passwords to prevent unauthorized tampering with the server setup. Passwords can restrict entry to the BIOS Setup, restrict use of the Boot Popup menu, and suppress automatic USB device reordering.

There is also an option to require a Power On password entry in order to boot the system. If the Power On Password function is enabled in Setup, the BIOS will halt early in POST to request a password before continuing POST.

Both Administrator and User passwords are supported by the BIOS. An Administrator password must be installed in order to set the User password. The maximum length of a password is 14 characters. A password can have alphanumeric (a-z, A-Z, 0-9) characters and it is case sensitive. Certain special characters are also allowed, from the following set:

<div align="center">

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

</div>

The Administrator and User passwords must be different from each other. An error message will be displayed if there is an attempt to enter the same password for one as for the other.

The use of *Strong Passwords* is encouraged, but not required. In order to meet the criteria for a Strong Password, the password entered must be at least 8 characters in length, and must include at least one each of alphabetic, numeric, and special characters. If a weak password is entered, a popup warning message will be displayed, although the weak password will be accepted.

Once set, a password can be cleared by changing it to a null string. This requires the Administrator password, and must be done through BIOS Setup or other explicit means of changing the passwords. Clearing the Administrator password will also clear the User password.

Alternatively, the passwords can be cleared by using the Password Clear jumper if necessary. Resetting the BIOS configuration settings to default values (by any method) has no effect on the Administrator and User passwords.

Entering the User password allows the user to modify only the System Time and System Date in the Setup Main screen. Other setup fields can be modified only if the Administrator password has been entered. If any password is set, a password is required to enter the BIOS setup.

The Administrator has control over all fields in the BIOS setup, including the ability to clear the User password and the Administrator password.

It is strongly recommended that at least an Administrator Password be set, since not having set a password gives everyone who boots the system the equivalent of administrative access. Unless an Administrator password is installed, any User can go into Setup and change BIOS settings at will.

In addition to restricting access to most Setup fields to viewing only when a User password is entered, defining a User password imposes restrictions on booting the system. In order to simply boot in the defined boot order, no password is required. However, the F6 Boot popup prompts for a password, and can only be used with the Administrator password. Also, when a User password is defined, it suppresses

the USB Reordering that occurs, if enabled, when a new USB boot device is attached to the system. A User is restricted from booting in anything other than the Boot Order defined in the Setup by an Administrator.

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, which also logs a SEL event to alert the authorized user or administrator that a password access failure has occurred.

## 4.2    Trusted Platform Module (TPM) Support

Trusted Platform Module (TPM) option is a hardware-based security device that addresses the growing concern on boot process integrity and offers better data protection. TPM protects the system start-up 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 1.2, by the Trusted Computing Group (TCG).

A TPM device is optionally installed onto a high density 14-pin connector labeled *TPM* 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 TPM to provide additional system and data security (for example, Microsoft Vista* supports Bitlocker drive encryption).

### 4.2.1    TPM security BIOS

The BIOS TPM support conforms to the *TPM PC Client Specific – Implementation Specification* for Conventional BIOS, version 1.2, and to the *TPM Interface Specification*, version 1.2. The BIOS adheres to the Microsoft Windows BitLocker* requirement. 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 EFI and legacy interfaces to a TPM-enabled operating system for using TPM.
- Produces 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, refer to the *TCG PC Client Specific Implementation Specification*, the *TCG PC Client Specific Physical Presence Interface Specification*, and the *Microsoft BitLocker\* Requirement* documents.

## 4.2.2        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. 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 commands, inhibits BIOS Setup entry, and boots directly to the operating system which requested the TPM commands.

## 4.2.3        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 BIOS TPM Setup, the operator can turn ON or OFF TPM functionality and clear the TPM ownership contents. After the requested TPM BIOS 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. Note that while using TPM, a TPM-enabled operating system or application may change the TPM state independent 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.

### 4.2.3.1        Security Screen

To enter the BIOS Setup, press the <F2> function key during boot time when the OEM or Intel® logo displays. The following message displays on the diagnostics screen and under the Quiet Boot logo screen:

> Press <F2> to enter setup

When the Setup is entered, the Main screen displays. The BIOS Setup utility provides the Security screen to enable and set the user and administrative passwords and to lock out the front panel buttons so they cannot be used. The Intel® Server Board S1200SP provides TPM settings through the security screen.

To access this screen from the Main screen, select the **Security** option.

| Main | Advanced | Security | Server Management | Boot Options | Boot Manager |
|------|----------|----------|-------------------|--------------|--------------|

| | |
|---|---|
| **Error! Reference source not found.** | <Installed/Not Installed> |
| **Error! Reference source not found.** | <Installed/Not Installed> |
| | |
| **Error! Reference source not found.** | [123aBcDeFgH$#@] |
| **Error! Reference source not found.** | [123aBcDeFgH$#@] |
| **Error! Reference source not found.** | Enabled/**Disabled** |
| | |
| **Error! Reference source not found.** | Enabled/**Disabled** |
| | |
| | |
| **Error! Reference source not found.** | <Displays current TPM Device State> |
| **Error! Reference source not found.** | **No Operation/**Turn On/Turn Off/Clear Ownership |

**Figure 16. Setup Utility – TPM Configuration Screen**

**Table 9. TPM Setup Utility – Security Configuration Screen Fields**

| Setup Item | Options | Help Text | Comments |
|---|---|---|---|
| TPM State* | Enabled and Activated<br>Enabled and Deactivated<br>Disabled and Activated<br>Disabled and Deactivated | | Information only.<br>Shows the current TPM device state.<br>A disabled TPM device will not execute commands that use TPM functions and TPM security operations will not be available.<br>An enabled and deactivated TPM is in the same state as a disabled TPM except setting of TPM ownership is allowed if not present already.<br>An enabled and activated TPM executes all commands that use TPM functions and TPM security operations will be available. |
| TPM Administrative Control** | **No Operation**<br>Turn On<br>Turn Off<br>Clear Ownership | [No Operation] – No changes to current state.<br>[Turn On] – Enables and activates TPM.<br>[Turn Off] – Disables and deactivates TPM.<br>[Clear Ownership] – Removes the TPM ownership authentication and returns the TPM to a factory default state. | Any Administrative Control operation selected will require the system to perform a Hard Reset in order to become effective. |

| Setup Item | Options | Help Text | Comments |
|---|---|---|---|
| | | **Note**: The BIOS setting returns to [No Operation] on every boot cycle by default. | |

## 4.3  Intel® Trusted Execution Technology

The Intel® Xeon® Processor E3-1200 v5 Product Family support Intel® Trusted Execution Technology (Intel® TXT), which is a robust security environment. Designed to help protect against software-based attacks, Intel® Trusted Execution Technology integrates new security features and capabilities into the processor, chipset, and other platform components. When used in conjunction with Intel® Virtualization Technology, Intel® Trusted Execution Technology provides hardware-rooted trust for your virtual applications.

This hardware-rooted security provides a general-purpose, safer computing environment capable of running a wide variety of operating systems and applications to increase the confidentiality and integrity of sensitive information without compromising the usability of the platform.

Intel® Trusted Execution Technology requires a computer system with Intel® Virtualization Technology enabled (both VT-x and VT-d), an Intel® Trusted Execution Technology-enabled processor, chipset, and BIOS, Authenticated Code Modules, and an Intel® Trusted Execution Technology compatible measured launched environment (MLE). The MLE could consist of a virtual machine monitor, an OS, or an application. In addition, Intel® Trusted Execution Technology requires the system to include a TPM v1.2, as defined by the *Trusted Computing Group TPM PC Client Specification*, Revision 1.2.

When available, Intel® Trusted Execution Technology can be enabled or disabled in the processor using a BIOS Setup option.

For general information about Intel® TXT, visit the Intel® Trusted Execution Technology website http://www.intel.com/technology/security/.

# 5.    Intel® Technology Support

## 5.1    Intel® Trusted Execution Technology

The Intel® Xeon® Processor E3-1200 v5 Product Family support Intel® Trusted Execution Technology (Intel® TXT), which is a robust security environment designed to help protect against software-based attacks. Intel® Trusted Execution Technology integrates new security features and capabilities into the processor, chipset, and other platform components. When used in conjunction with Intel® Virtualization Technology and Intel® VT for Directed IO, with an active TPM, Intel® Trusted Execution Technology provides hardware-rooted trust for your virtual applications.

## 5.2    Intel® Virtualization Technology – Intel® VT-x/VT-d/VT-c

Intel® Virtualization Technology consists of three components which are integrated and interrelated, but which address different areas of Virtualization.

- Intel® Virtualization Technology (VT-x) is processor-related and provides capabilities needed to provide hardware assist to a Virtual Machine Monitor (VMM).
- Intel® Virtualization Technology for Directed I/O (VT-d) is primarily concerned with virtualizing I/O efficiently in a VMM environment. This would generally be a chipset I/O feature, but in the Second Generation Intel® Core™ Processor Family there is an Integrated I/O unit embedded in the processor, and the IIO is also enabled for VT-d.
- Intel® Virtualization Technology for Connectivity (VT-c) is primarily concerned I/O hardware assist features, complementary to but independent of VT-d.

Intel® VT-x is designed to support multiple software environments sharing same hardware resources. Each software environment may consist of OS and applications. The Intel® Virtualization Technology features can be enabled or disabled in the BIOS setup. The default behavior is disabled.

Intel® VT-d is supported jointly by the Intel® Xeon® Processor E3-1200 V5 Product Families and The Intel® C230 series chipset. Both support DMA remapping from inbound PCI Express* memory Guest Physical Address (GPA) to Host Physical Address (HPA). PCI devices are directly assigned to a virtual machine leading to a robust and efficient virtualization.

The Intel® S1200SP Server Board Family BIOS publishes the DMAR table in the ACPI Tables. For each DMA Remapping Engine in the platform, one exact entry of DRHD (DMA Remapping Hardware Unit Definition) structure is added to the DMAR. The DRHD structure in turn contains a Device Scope structure that describes the PCI endpoints and/or sub-hierarchies handled by the particular DMA Remapping Engine.

Similarly, there are reserved memory regions typically allocated by the BIOS at boot time. The BIOS marks these regions as either reserved or unavailable in the system address memory map reported to the OS. Some of these regions can be a target of DMA requests from one or more devices in the system, while the OS or executive is active. The BIOS reports each such memory region using exactly one RMRR (Reserved Memory Region Reporting) structure in the DMAR. Each RMRR has a Device Scope listing the devices in the system that can cause a DMA request to the region.

For more information on the DMAR table and the DRHD entry format, refer to the *Intel® Virtualization Technology for Directed I/O Architecture Specification*. For more general information about VT-x, VT-d, and VT-c, a good reference is *Enabling Intel® Virtualization Technology Features and Benefits White Paper*.

## 5.3    Intel® Intelligent Power Node Manager

Data centers are faced with power and cooling challenges that are driven by increasing numbers of servers deployed and server density in the face of several data center power and cooling constraints. In this type of environment, Information Technology (IT) needs the ability to monitor actual platform power consumption and control power allocation to servers and racks in order to solve specific data center problems including the following issues.

**Table 10. Intel® Intelligent Power Node Manager**

| IT Challenge | Requirement |
|---|---|
| Over-allocation of power | <ul><li>Ability to monitor actual power consumption</li><li>Control capability that can maintain a power budget to enable dynamic power allocation to each server</li></ul> |
| Under-population of rack space | Control capability that can maintain a power budget to enable increased rack population |
| High energy costs | Control capability that can maintain a power budget to ensure that a set energy cost can be achieved |
| Capacity planning | <ul><li>Ability to monitor actual power consumption to enable power usage modeling over time and a given planning period</li><li>Ability to understand cooling demand from a temperature and airflow perspective</li></ul> |
| Detection and correction of hot spots | <ul><li>Control capability that reduces platform power consumption to protect a server in a hot-spot</li><li>Ability to monitor server inlet temperatures to enable greater rack utilization in areas with adequate cooling</li></ul> |

The requirements listed above are those that are addressed by the Intel® C230 series chipset Management Engine (ME) and Intel® Intelligent Power Node Manager (NM) technology. The ME/NM combination is a power and thermal control capability on the platform, which exposes external interfaces that allow IT (through external management software) to query the ME about platform power capability and consumption, thermal characteristics, and specify policy directives (for example, set a platform power budget).

Node Manager (NM) is a platform resident technology that enforces power capping and thermal-triggered power capping policies for the platform. These policies are applied by exploiting subsystem knobs (such as processor P and T states) that can be used to control power consumption. NM enables data center power management by exposing an external interface to management software through which platform policies can be specified. It also implements specific data center power management usage models such as power limiting and thermal monitoring.

The NM feature is implemented by a complementary architecture utilizing the ME, BMC, BIOS, and an ACPI-compliant OS. The ME provides the NM policy engine and power control/limiting functions (referred to as Node Manager or NM) while the BMC provides the external LAN link by which external management software can interact with the feature. The BIOS provides system power information utilized by the NM

algorithms and also exports ACPI Source Language (ASL) code used by OS-Directed Power Management (OSPM) for negotiating processor P and T state changes for power limiting. PMBus*-compliant power supplies provide the capability to monitoring input power consumption, which is necessary to support NM.

Following are the some of the applications of Intel® Intelligent Power Node Manager technology:

- **Platform Power Monitoring and Limiting**: The ME/NM monitors platform power consumption and holds average power over duration. It can be queried to return actual power at any given instance. The power limiting capability is to allow external management software to address key IT issues by setting a power budget for each server. For example, if there is a physical limit on the power available in a room, IT can decide to allocate power to different servers based on their usage – servers running critical systems can be allowed more power than servers that are running less critical workload.

- **Inlet Air Temperature Monitoring**: The ME/NM monitors server inlet air temperatures periodically. If there is an alert threshold in effect, ME/NM issues an alert when the inlet (room) temperature exceeds the specified value. The threshold value can be set by policy.

- **Memory Subsystem Power Limiting**: The ME/NM monitors memory power consumption. Memory power consumption is estimated using average bandwidth utilization information

- **Processor Power monitoring and limiting**: The ME/NM monitors processor or socket power consumption and holds average power over duration. It can be queried to return actual power at any given instant. The monitoring process of the ME will be used to limit the processor power consumption through processor P-states and dynamic core allocation.

- **Core allocation at boot time**: Restrict the number of cores for OS/VMM use by limiting how many cores are active at boot time. After the cores are turned off, the CPU will limit how many working cores are visible to BIOS and OS/VMM. The cores that are turned off cannot be turned on dynamically after the OS has started. It can be changed only at the next system reboot.

- **Core allocation at run-time**: This particular use case provides a higher level processor power control mechanism to a user at run-time, after booting. An external agent can dynamically use or not use cores in the processor subsystem by requesting ME/NM to control them, specifying the number of cores to use or not use.

**Table 11. Intel® Intelligent Power Node Manager Capabilities and Features (SPS 4.x)**

| Value Vector | Capabilities and Features | SPS 4.x |
|---|---|---|
| Node Mgr API | ACPI power meter support | ✓ |
| | DCMI API support | ✓ |
| | Node Manager IPMI API support | ✓ |
| | ACPI support | ✓ |
| Monitoring | Platform power telemetry (per node, in multi-node systems) | ✓ |
| | CPU and Memory power telemetry | ✓ |
| | Support voltage regulators & current monitor configuration | ✓ |
| | PMBus 1.2 support | ✓ |
| | BMC power readings support | ✓ |
| | Hot-swap controller support | ✓ |

| Value  Vector | Capabilities and Features | SPS 4.x |
|---|---|---|
| | Shared power supply support consistent with SPS 2.0 (Romley) | ✓ |
| Limiting | Platform-level policy limits (16 policies) | ✓ |
| | Boot mode selection | |
| | Core disable | ✓ |
| | Power limit during boot | ✓ |
| | Running average power limit | ✓ |
| | Dynamic core allocation | ✓ |
| Hardware Protection | SMART/CLST | ✓ |
| Performance & Characterization | Node Mgr Power Thermal Utility (PTU) | ✓ |

## 5.3.1     Hardware Requirements

NM is supported only on platforms that have the NM FW functionality loaded and enabled on the Management Engine (ME) in the SSB and that have a BMC present to support the external LAN interface to the ME. NM power limiting feature requires a means for the ME to monitor input power consumption for the platform. This capability is generally provided by means of PMBus*-compliant power supplies although an alternative model using a simpler SMBus* power monitoring device is possible (there is potential loss in accuracy and responsiveness using non-PMBus* devices). The NM SmaRT/CLST feature requires specific PMBus*-compliant power supplies as well as additional hardware on the baseboard.

# 6. Platform Management Functional Overview

Platform management functionality is supported by several hardware and software components integrated on the server board that work together to control system functions, monitor and report system health, and control various thermal and performance features in order to maintain (when possible) server functionality in the event of component failure and/or environmentally stressed conditions.

This chapter provides a high level overview of the platform management features and functionality implemented on the server board. For more in depth and design level Platform Management information, refer to the *BMC Core Firmware External Product Specification (EPS)* and *BIOS Core External Product Specification (EPS)* for Intel® Server products based on the Intel® Xeon® processor E3-1200 V5 product family.

## 6.1 Baseboard Management Controller (BMC) Firmware Feature Support

The following sections outline features that the integrated BMC firmware can support. Support or utilization for some features is dependent on the server platform in which the server board is integrated and any additional system level components and options that may be installed.

### 6.1.1 IPMI 2.0 Features

- Baseboard management controller (BMC)
- IPMI Watchdog timer
- Messaging support, including command bridging and user/session support
- Chassis device functionality, including power/reset control and BIOS boot flags support
- Event receiver device: The BMC receives and processes events from other platform subsystems.
- Field Replaceable Unit (FRU) inventory device functionality: The BMC supports access to system FRU devices using IPMI FRU commands.
- System Event Log (SEL) device functionality: The BMC supports and provides access to a SEL.
- Sensor Data Record (SDR) repository device functionality: The BMC supports storage and access of system SDRs.
- Sensor device and sensor scanning/monitoring: The BMC provides IPMI management of sensors. It polls sensors to monitor and report system health.
- IPMI interfaces
  - Host interfaces including system management software (SMS) with receive message queue support, and server management mode (SMM)
  - IPMB interface
  - LAN interface that supports the IPMI-over-LAN protocol Remote Management Control Protocol (RMCP, RMCP+)
- Serial-over-LAN (SOL)
- ACPI state synchronization: The BMC tracks ACPI state changes that are provided by the BIOS.
- BMC self-test: The BMC performs initialization and run-time self-tests and makes results available to external entities.

See also the *Intelligent Platform Management Interface Specification Second Generation v2.0.*

## 6.1.2 Non-IPMI Features

The BMC supports the following non-IPMI features. This list does not preclude support for future enhancements or additions.

- In-circuit BMC firmware update
- Fault resilient booting (FRB): FRB2 is supported by the watchdog timer functionality.
- Chassis intrusion detection
- Basic fan speed control using Control version 2 SDRs
- Fan redundancy monitoring and support
- Power supply redundancy monitoring and support
- Hot-swap fan support
- Acoustic management: Support for multiple fan profiles
- Signal testing support: The BMC provides test commands for setting and getting platform signal states.
- The BMC generates diagnostic beep codes for fault conditions.
- System GUID storage and retrieval
- Front panel management: 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.
- Power state retention
- Power fault analysis
- Intel® Light-Guided Diagnostics
- Power unit management: Support for power unit sensor. The BMC handles power-good dropout conditions.
- DIMM temperature monitoring: New sensors and improved acoustic management using closed-loop fan control algorithm taking into account DIMM temperature readings.
- Address Resolution Protocol (ARP): The BMC sends and responds to ARPs (supported on embedded NICs).
- Dynamic Host Configuration Protocol (DHCP): The BMC performs DHCP (supported on embedded NICs).
- Platform environment control interface (PECI) thermal management support
- E-mail alerting
- Embedded web server:
- Integrated KVM
- Integrated Remote Media Redirection
- Lightweight Directory Access Protocol (LDAP) support
- Intel® Intelligent Power Node Manager support

## 6.2    Basic and Advanced Features

The following table lists basic and advanced feature support. Individual features may vary by platform. See the appropriate Platform Specific EPS addendum for more information.

**Table 12. Basic and Advanced Features**

| Feature | Basic* | Advanced** |
|---|---|---|
| IPMI 2.0 Feature Support | Yes | Yes |
| In-circuit BMC Firmware Update | Yes | Yes |
| FRB 2 | Yes | Yes |
| Chassis Intrusion Detection | Yes | Yes |
| Fan Redundancy Monitoring | Yes | Yes |
| Hot-Swap Fan Support | Yes | Yes |
| Acoustic Management | Yes | Yes |
| Diagnostic Beep Code Support | Yes | Yes |
| Power State Retention | Yes | Yes |
| ARP/DHCP Support | Yes | Yes |
| PECI Thermal Management Support | Yes | Yes |
| E-mail Alerting | Yes | Yes |
| Embedded Web Server | Yes | Yes |
| SSH Support | Yes | Yes |
| Integrated KVM | | Yes |
| Integrated Remote Media Redirection | | Yes |
| Lightweight Directory Access Protocol (LDAP) | Yes | Yes |
| Intel® Intelligent Power Node Manager Support*** | Yes | Yes |
| SMASH CLP | Yes | Yes |

* Basic management features provided by Integrated BMC

**Advanced management features available with optional Intel® Remote Management Module 4

*** Intel® Intelligent Power Node Manager Support requires PMBus*-compliant power supply

## 6.3    Advanced Configuration and Power Interface (ACPI)

The server board supports the following ACPI states.

**Table 13. ACPI Power States**

| State | Supported | Description |
|---|---|---|
| S0 | Yes | Working<br>▪ The front panel power LED is on (not controlled by the BMC).<br>▪ The fans spin at the normal speed, as determined by sensor inputs.<br>▪ Front panel buttons work normally. |
| S1 | No | Not supported |
| S2 | No | Not supported |

| State | Supported | Description |
|---|---|---|
| S3 | No | Supported only on Workstation platforms. See appropriate Platform Specific Information for more information. |
| S4 | No | Not supported |
| S5 | Yes | Soft off<br>▪ The front panel buttons are not locked.<br>▪ The fans are stopped.<br>▪ The power-up process goes through the normal boot process.<br>▪ The power, reset, front panel NMI, and ID buttons are unlocked. |

## 6.4  Power Control Sources

The server board supports several power control sources which can initiate a power-up or power-down activity.

### Table 14. Power Control Initiators

| Source | External Signal Name or Internal Subsystem | Capabilities |
|---|---|---|
| Power button | Front panel power button | Turns power on or off |
| BMC watchdog timer | Internal BMC timer | Turns power off, or power cycle |
| Command | Routed through command processor | Turns power on or off, or power cycle |
| Power state retention | Implemented by means of BMC internal logic | Turns power on when AC power returns |
| Chipset | Sleep S4/S5 signal (same as *POWER_ON*) | Turns power on or off |
| CPU Thermal | CPU Thermtrip | Turns power off |
| WOL(Wake On LAN) | LAN | Turns power on |
| PCH Thermal | PCH Thermtrip | Pops up warning message.<br>Turns power off when temperature has cross the threshold |
| Fan and Temperature | Fan failure and temperature critical | Turns power off * |
| Power Supply | Power Supply Over Current/Over Temperature | Turns power off * ** |

* Not applicable to all products. Applies only to Multi-Node products.

** Not applicable to all products. Applies only to Node3 and Node4 on Multi-Node products when the Shutdown policy feature is enabled.

## 6.5  BMC Watchdog

The BMC FW is increasingly called upon to perform system functions that are time-critical in that failure to provide these functions in a timely manner can result in system or component damage. Intel® server board S1200SP introduces a BMC watchdog feature to provide a safe-guard against this scenario by providing an automatic recovery mechanism. It also can provide automatic recovery of functionality that has failed due to a fatal FW defect triggered by a rare sequence of events or a BMC hang due to some type of HW glitch (for example, power).

This feature is comprised of a set of capabilities whose purpose is to detect misbehaving subsections of BMC firmware, the BMC CPU itself, or HW subsystems of the BMC component, and to take appropriate action to restore proper operation. The action taken is dependent on the nature of the detected failure and may result in a restart of the BMC CPU, one or more BMC HW subsystems, or a restart of malfunctioning FW subsystems.

- The BMC watchdog feature is designed to provide protection against the problems listed below regardless of the state of the BMC FW and BMC component's internal HW when the problem is detected.
- Linux* "kernel panic" – Results in reset of the entire FW stack (see Note1 below).
- Hangs in individual threads/processes – Offending process may be reset or entire FW stack reset may be required.
- BMC CPU and/or BMC HW subsystems going into a faulted or unusable state due to triggers external to the BMC component (for example, power glitches) – HW watchdog may be used to reset the BMC CPU and/or affected BMC HW subsystems.
- Low or out-of-memory condition – The platform management subsystem will reset itself upon detection of this condition.

The BMC watchdog feature only allows up to three resets of the BMC CPU (such as HW reset) or entire FW stack (such as a SW reset) before giving up and remaining in the uBOOT code. This count is cleared upon cycling of power to the BMC or upon continuous operation of the BMC without a watchdog-generated reset occurring for a period of greater than 30 minutes. The BMC FW logs a SEL event indicating that a watchdog-generated BMC reset (either soft or hard reset) has occurred. This event may be logged after the actual reset has occurred. Refer to sensor section for details for the related sensor definition. The BMC will also indicate a degraded system status on the Front Panel Status LED after a BMC HW reset or FW stack reset. This state (which follows the state of the associated sensor) will be cleared upon system reset or (AC or DC) power cycle.

*Note: A reset of the BMC may result in the following system degradations that will require a system reset or power cycle to correct:*

1. *Timeout value for the rotation period can be set using this parameter. Potentially, there will be incorrect ACPI Power State reported by the BMC.*

2. *Reversion of temporary test modes for the BMC back to normal operational modes.*

3. *FP status LED and DIMM fault LEDs may not reflect BIOS detected errors.*

## 6.6    Fault Resilient Booting (FRB)

Fault resilient booting (FRB) is a set of BIOS and BMC algorithms and hardware support that allow a multiprocessor system to boot even if the bootstrap processor (BSP) fails. Only FRB2 is supported using watchdog timer commands.

FRB2 refers to the FRB algorithm that detects system failures during POST. The BIOS uses the BMC watchdog timer to back up its operation during POST. The BIOS configures the watchdog timer to indicate that the BIOS is using the timer for the FRB2 phase of the boot operation.

After the BIOS has identified and saved the BSP information, it sets the FRB2 timer use bit and loads the watchdog timer with the new timeout interval.

If the watchdog timer expires while the watchdog use bit is set to FRB2, the BMC (if so configured) logs a watchdog expiration event showing the FRB2 timeout in the event data bytes. The BMC then hard resets the system, assuming the BIOS-selected reset as the watchdog timeout action.

The BIOS is responsible for disabling the FRB2 timeout before initiating the option ROM scan and before displaying a request for a boot password. If the processor fails and causes an FRB2 timeout, the BMC resets the system.

The BIOS gets the watchdog expiration status from the BMC. If the status shows an expired FRB2 timer, the BIOS enters the failure in the system event log (SEL). In the OEM bytes entry in the SEL, the last POST code generated during the previous boot attempt is written. FRB2 failure is not reflected in the processor status sensor value.

The FRB2 failure does not affect the front panel LEDs.

## 6.7   Sensor Monitoring

The BMC monitors system hardware and reports system health. Some of the sensors include those for monitoring:

- Component, board, and platform temperatures
- Board and platform voltages
- System fan presence and tach
- Chassis intrusion
- Front Panel NMI
- Front Panel Power and System Reset Buttons
- SMI timeout
- Processor errors

The information gathered from physical sensors is translated into IPMI sensors as part of the IPMI Sensor Model. The BMC also reports various system state changes by maintaining virtual sensors that are not specifically tied to physical hardware.

See *Appendix B – Integrated BMC Sensor Tables* for additional sensor information.

## 6.8   Field Replaceable Unit (FRU) Inventory Device

The BMC implements the interface for logical FRU inventory devices as specified in the *Intelligent Platform Management Interface Specification*, Version 2.0. This functionality provides commands used for accessing and managing the FRU inventory information. These commands can be delivered through all interfaces.

The BMC provides FRU device command access to its own FRU device and to the FRU devices throughout the server. The FRU device ID mapping is defined in the Platform Specific Information. The BMC controls the mapping of the FRU device ID to the physical device.

## 6.9    System Event Log (SEL)

The BMC implements the system event log as specified in the *Intelligent Platform Management Interface Specification*, Version 2.0. The SEL is accessible regardless of the system power state through the BMC's in-band and out-of-band interfaces.

The BMC allocates 95231bytes (approx. 93 KB) of non-volatile storage space to store system events. The SEL timestamps may not be in order. Up to 3,638 SEL records can be stored at a time. Because the SEL is circular, any command that results in an overflow of the SEL beyond the allocated space will overwrite the oldest entries in the SEL, while setting the overflow flag.

Events logged to the SEL can be viewed using Intel's SELVIEW utility, Embedded Web Server, and Active System Console.

## 6.10  System Fan Management

The BMC controls and monitors the system fans. Each fan is associated with a fan speed sensor that detects fan failure and may also be associated with a fan presence sensor for hot-swap support. For redundant fan configurations, the fan failure and presence status determines the fan redundancy sensor state.

The system fans are divided into fan domains, each of which has a separate fan speed control signal and a separate configurable fan control policy. A fan domain can have a set of temperature and fan sensors associated with it. These are used to determine the current fan domain state.

A fan domain has three states: sleep, nominal, and boost. The sleep and boost states have fixed (but configurable through OEM SDRs) fan speeds associated with them. The nominal state has a variable speed determined by the fan domain policy. An OEM SDR record is used to configure the fan domain policy.

The fan domain state is controlled by several factors. They are listed below in order of precedence, high to low:

- Boost
    - o  Associated fan is in a critical state or missing. The SDR describes which fan domains are boosted in response to a fan failure or removal in each domain. If a fan is removed when the system is in 'Fans-off' mode it will not be detected and there will not be any fan boost till system comes out of 'Fans-off; mode.
    - o  Any associated temperature sensor is in a critical state. The SDR describes which temperature-threshold violations cause fan boost for each fan domain.
    - o  The BMC is in firmware update mode, or the operational firmware is corrupted.
    - o  If any of the above conditions apply, the fans are set to a fixed boost state speed.
- Nominal
    - o  A fan domain's nominal fan speed can be configured as static (fixed value) or controlled by the state of one or more associated temperature sensors.
    - o  Hysteresis can be specified to minimize fan speed oscillation and to smooth fan speed transitions.

### 6.10.1    Thermal and Acoustic Management

This feature refers to enhanced fan management to keep the system optimally cooled while reducing the amount of noise generated by the system fans. Aggressive acoustics standards might require a trade-off between fan speed and system performance parameters that contribute to the cooling requirements, primarily memory bandwidth. The BIOS, BMC, and SDRs work together to provide control over how this trade-off is determined.

This capability requires the BMC to access temperature sensors on the individual memory DIMMs.

## 6.10.2    Thermal Sensor Input to Fan Speed Control

The BMC uses various IPMI sensors as input to the fan speed control. Some of the sensors are IPMI models of actual physical sensors whereas some are virtual sensors whose values are derived from physical sensors using calculations and/or tabular information.

The following IPMI thermal sensors are used as input to the fan speed control:

- Front Panel Temperature Sensor[1]
- CPU Margin Sensors[2,4,5]
- DIMM Thermal Margin Sensors[2,4]
- Exit Air Temperature Sensor[1, 7, 9]
- PCH Temperature Sensor[3,5]
- Add-In Intel SAS Module Temperature Sensors[3, 5]
- PSU Thermal Sensor[3, 8]
- CPU VR Temperature Sensors[3, 6]
- DIMM VR Temperature Sensors[3, 6]
- BMC Temperature Sensor[3, 6]
- Global Aggregate Thermal Margin Sensors[7]
- Hot Swap Backplane Temperature Sensors
- I/O module Temperature Sensor (With option installed)
- Intel® ROC Module (With option installed)
- Riser Card Temperature Sensors
- Intel® Xeon Phi™ coprocessor (With option installed)

*Notes:*

1. *For fan speed control in Intel® chassis*

2. *Temperature margin from throttling threshold*

3. *Absolute temperature*

4. *PECI value or margin value*

5. *On-die sensor*

6. *On-board sensor*

7. *Virtual sensor*

8. *Available only when PSU has PMBus*

9. *Calculated estimate*

The following illustration provides a simple model showing the fan speed control structure that implements the resulting fan speeds.
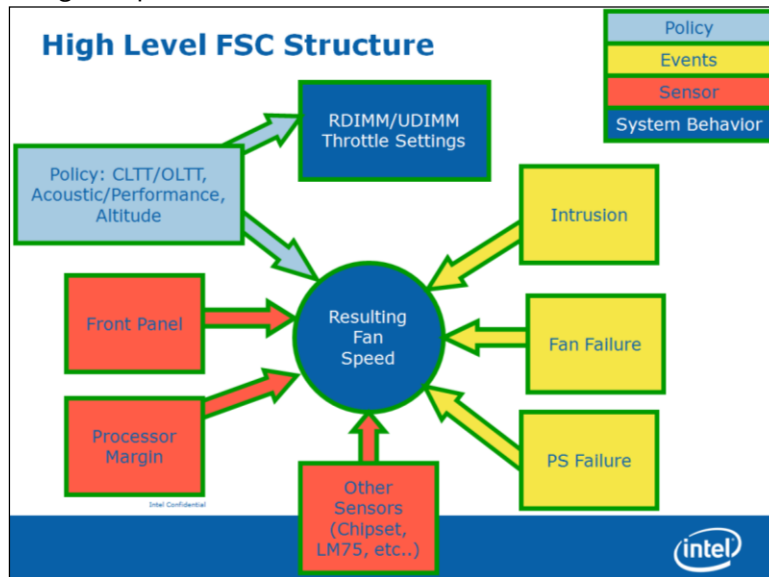


**Figure 17. Fan Speed Control Process**

### 6.10.3    Auto Profiles

PCSD board implements auto profile feature to improve upon previous platform configuration-dependent FSC and maintain competitive acoustics within the market. This feature is not available for third party customization.

BIOS and BMC will handshake to automatically understand configuration details and automatically select the optimal fan speed control profile in the BMC.

Customers will only select a performance or an acoustic profile selection from the BIOS menu for EPSD system and the fan speed control will be optimal for the configuration loaded.

There will be no manual selection of profiles at different altitudes, but altitude impact will be well covered by auto profile.

Users can still choose performance or acoustic profile in BIOS setting. Default is acoustic. Performance option is recommended if customer installs M.2 SSD or any other PCI-e add-in cards which requires excessive cooling, e.g., boundary condition of 55C and 300LFM.

To support PCI-e add-in cards:

- ▪ Acoustic option is targeted to meet boundary condition of 55C&200LFM.

- ▪ Performance option is targeted to meet boundary condition beyond 55C&200LFM. e.g., boundary condition of 55C and 300LFM.

### 6.10.4    Memory Thermal Throttling

The system shall support thermal management through static closed loop throttling (Static-CLTT) of system memory based on the platform as well as availability of valid temperature sensors on the installed memory DIMMs. Throttling levels are changed dynamically to cap throttling based on memory and system thermal conditions as determined by the system and DIMM power and thermal parameters. Support for CLTT on mixed-mode DIMM populations (that is, some installed DIMMs have valid temp sensors and some do not) is not supported. The BMC fan speed control functionality is related to the memory throttling mechanism used.

The following terminology is used for the various memory throttling options:

- **Static Closed Loop Thermal Throttling (Static-CLTT)**: CLTT control registers are configured by BIOS MRC during POST. The memory throttling is run as a closed-loop system with the DIMM temperature sensors as the control input. Otherwise, the system does not change any of the throttling control registers in the embedded memory controller during runtime.

- Intel® Server Systems supporting the Intel® Xeon® processor E3-1200 v5 product family introduce a new type of CLTT which is referred to as Hybrid CLTT for which the Integrated Memory Controller estimates the DRAM temperature in between actual reads of the TSODs. Hybrid CLTTT shall be used on all Intel® Server Systems supporting the Intel® Xeon® processor E3-1200 v5 product family that have DIMMs with thermal sensors. Therefore, the terms Dynamic-CLTT and Static-CLTT are really referring to this 'hybrid' mode. Note that if the IMC's polling of the TSODs is interrupted, the temperature readings that the BMC gets from the IMC shall be these estimated values.

## 6.11 Messaging Interfaces

The BMC supports the following communications interfaces:

- Host SMS interface by means of low pin count (LPC)/keyboard controller style (KCS) interface

- Host SMM interface by means of low pin count (LPC)/keyboard controller style (KCS) interface

- Intelligent Platform Management Bus (IPMB) I2C interface

- LAN interface using the IPMI-over-LAN protocols

Every messaging interface is assigned an IPMI channel ID by IPMI 2.0. The following table shows the standard channel assignments.

**Table 15. Messaging Interfaces**

| Channel ID | Interface | Supports Sessions |
|---|---|---|
| 0 | Primary IPMB | No |
| 1 | LAN 1 | Yes |
| 2 | LAN 2 | Yes |
| 3 | LAN3[1] (Provided by the Intel® Dedicated Server Management NIC) | Yes |
| 4 | Reserved | Yes |
| 5 | USB[2] | No |
| 6 | Secondary IPMB | No |
| 7 | SMM | No |
| 8 – 0Dh | Reserved | – |
| 0Eh | Self[3] | – |
| 0Fh | SMS/Receive Message Queue | No |

*Notes:*

1. *Optional hardware supported by the server system.*

*2. Reserve USB channel number, current BMC firmware does not support communication through a USB channel.*

*3. Refers to the actual channel used to send the request.*

## 6.11.1    User Model

The BMC supports the IPMI 2.0 user model. 15 user IDs are supported. These 15 users can be assigned to any channel. The following restrictions are placed on user-related operations:

1. User names for User IDs 1 and 2 cannot be changed. These are always "" (Null/blank) and "root" respectively.
2. User 2 ("root") always has the administrator privilege level.
3. All user passwords (including passwords for 1 and 2) may be modified.

4. User IDs 3-15 may be used freely, with the condition that user names are unique. Therefore, no other users can be named "" (Null), "root," or any other existing user name.

## 6.11.2    IPMB Communication Interface

The IPMB communication interface uses the 100 KB/s version of an I$^2$C bus as its physical medium. For more information on I$^2$C specifications, see *The I$^2$C Bus and How to Use It*. The IPMB implementation in the BMC is compliant with the *IPMB v1.0*, revision 1.0.

The BMC IPMB slave address is 20h.

The BMC both sends and receives IPMB messages over the IPMB interface. Non-IPMB messages received by means of the IPMB interface are discarded.

Messages sent by the BMC can either be originated by the BMC, such as initialization agent operation, or by another source. One example is KCS-IPMB bridging.

## 6.11.3    LAN Interface

The BMC implements both the IPMI 1.5 and IPMI 2.0 messaging models. These provide out-of-band local area network (LAN) communication between the BMC and the network.

See the *Intelligent Platform Management Interface Specification Second Generation v2.0* for details about the IPMI-over-LAN protocol.

Run-time determination of LAN channel capabilities can be determined by both standard IPMI defined mechanisms.

### 6.11.3.1      RMCP/ Alert Standards Forum (ASF Messaging)

The BMC supports RMCP ping discovery in which the BMC responds with a pong message to an RMCP/ASF ping request. This is implemented per the *Intelligent Platform Management Interface Specification Second Generation v2.0*.

### 6.11.3.2 BMC LAN Channels

The BMC supports three RMII/RGMII ports that can be used for communicating with Ethernet devices. Two ports are used for communication with the on-board NICs and one is used for communication with an Ethernet PHY located on the onboard dedicated RMM4 NIC.

#### 6.11.3.2.1 Baseboard NICs

The on-board Ethernet controller provides support for a Network Controller Sideband Interface (NC-SI) manageability interface. This provides a sideband high-speed connection for manageability traffic to the BMC while still allowing for a simultaneous host access to the OS if desired.

The NC-SI is a DMTF industry standard protocol for the side band management LAN interface. This protocol provides a fast multi-drop interface for management traffic.

The baseboard NICs are connected to a single BMC RMII/RGMII port that is configured for RMII operation. The NC-SI protocol is used for this connection and provides a 100 Mb/s full-duplex multi-drop interface which allows multiple NICs to be connected to the BMC. The physical layer is based upon RMII, however RMII is a point-to-point bus whereas NC-SI allows 1 master and up to 4 slaves. The logical layer (configuration commands) is incompatible with RMII.

The server board provides support for a dedicated management channel that can be configured to be hidden from the host and only used by the BMC. This mode of operation is configured using a BIOS setup option.

#### 6.11.3.2.2 Dedicated Management Channel

An additional LAN channel dedicated to BMC usage is supported using the on-board RMM4 NIC. The BMC has a built-in MAC module that uses the RGMII interface to link with the RMM4 NIC's PHY. Therefore, for this dedicated management interface, the PHY and MAC are located in different devices.

The PHY on the RMM4 connects to the BMC's other RMII/RGMII interface (that is, the one that is not connected to the baseboard NICs). This BMC port is configured for RGMII usage.

In addition to the use of the on-board dedicated RMM4 NIC for a dedicated management channel, on systems that support multiple Ethernet ports on the baseboard, the system BIOS provides a setup option to allow one of these baseboard ports to be dedicated to the BMC for manageability purposes. When this is enabled, that port is hidden from the OS. By default, this interface is disabled and must be configured via the BIOS, EWS, or IPMI commands.

#### 6.11.3.2.3 Concurrent Server Management Use of Multiple Ethernet Controllers

The BMC FW supports concurrent OOB LAN management sessions for the following combination:

- 2 on-board NIC ports
- 1 on-board NIC and the on-board dedicated RMM4 NIC
- 2 on-board NICs and the on-board dedicated RMM4 NIC

All NIC ports must be on different subnets for the concurrent usage models above.

MAC addresses are assigned for management NICs from a pool of up to 3 MAC addresses allocated specifically for manageability.

The server board has seven MAC addresses programmed at the factory. MAC addresses are assigned as follows:

- NIC 1 MAC address (for OS usage)
- NIC 2 MAC address = NIC 1 MAC address + 1 (for OS usage)
- BMC LAN channel 1 MAC address = NIC1 MAC address + 2
- BMC LAN channel 2 MAC address = NIC1 MAC address + 3
- BMC LAN channel 3 (RMM4) MAC address = NIC1 MAC address + 4

The printed MAC address on the server board and/or server system is assigned to NIC1 on the server board.

For security reasons, embedded LAN channels have the following default settings:

- IP Address: Static
- All users disabled

IPMI-enabled network interfaces may not be placed on the same subnet. This includes the Intel® Dedicated Server Management NIC and either of the BMC's embedded network interfaces.

Host-BMC communication over the same physical LAN connection – also known as *loopback* – is not supported. This includes *ping* operations.

On server boards with more than two onboard NIC ports, only the first two ports can be used as BMC LAN channels. The remaining ports have no BMC connectivity.

Maximum bandwidth supported by BMC LAN channels are as follows:

- BMC LAN1 (Baseboard NIC port) – 100Mb (10Mb in DC off state)
- BMC LAN 2 (Baseboard NIC port) – 100Mb (10Mb in DC off state)
- BMC LAN 3 (Dedicated NIC) – 1000Mb

### 6.11.3.3 IPV6 Support

In addition to IPv4, the server board supports IPv6 for manageability channels. Configuration of IPv6 is provided by extensions to the IPMI Set and Get LAN Configuration Parameters commands as well as through a Web Console IPv6 configuration web page.

The BMC supports IPv4 and IPv6 simultaneously so they are both configured separately and completely independently. For example, IPv4 can be DHCP configured while IPv6 is statically configured or vice versa.

The parameters for IPv6 are similar to the parameters for IPv4 with the following differences:

- An IPv6 address is 16 bytes vs. 4 bytes for IPv4.
- An IPv6 prefix is 0 to 128 bits whereas IPv4 has a 4 byte subnet mask.
- The IPv6 Enable parameter must be set before any IPv6 packets are sent or received on that channel.
- There are two variants of automatic IP Address Source configuration vs. just DHCP for IPv4.

The three possible IPv6 IP Address Sources for configuring the BMC are:

- **Static (Manual)**: The IP, Prefix, and Gateway parameters are manually configured by the user. The BMC ignores any Router Advertisement messages received over the network.

- **DHCPv6**: The IP comes from running a DHCPv6 client on the BMC and receiving the IP from a DHCPv6 server somewhere on the network. The Prefix and Gateway are configured by Router Advertisements from the local router. The IP, Prefix, and Gateway are read-only parameters to the BMC user in this mode.

- **Stateless auto-config**: The Prefix and Gateway are configured by the router through Router Advertisements. The BMC derives its IP in two parts: the upper network portion comes from the router and the lower unique portion comes from the BMC's channel MAC address. The 6-byte MAC address is converted into an 8-byte value per the EUI-64* standard. For example, a MAC value of *00:15:17:FE:2F:62* converts into a EUI-64 value of *215:17ff:fefe:2f62*. If the BMC receives a Router Advertisement from a router at IP *1:2:3:4::1* with a prefix of 64, it would then generate for itself an IP of *1:2:3:4:215:17ff:fefe:2f62*. The IP, Prefix, and Gateway are read-only parameters to the BMC user in this mode.

IPv6 can be used with the BMC's Web Console, JViewer* (remote KVM and Media), and Systems Management Architecture for Server Hardware – Command Line Protocol (SMASH-CLP) interface (SSH). There is no standard yet on how IPMI RMCP or RMCP+ should operate over IPv6 so that is not currently supported.

### 6.11.3.4    LAN Failover

The BMC FW provides a LAN failover capability so that the failure of the system HW associated with one LAN link will result in traffic being rerouted to an alternate link. This functionality is configurable using IPMI methods as well as the BMC's Embedded UI, allowing for user to specify the physical LAN links constitute the redundant network paths or physical LAN links constitute different network paths. BMC supports only an *all or nothing* approach – that is, all interfaces bonded together, or none are bonded together.

The LAN Failover feature applies only to BMC LAN traffic. It bonds all available Ethernet devices but only one is active at a time. When enabled, if the active connection's leash is lost, one of the secondary connections is automatically configured so that it has the same IP address. Traffic immediately resumes on the new active connection.

The LAN Failover enable/disable command may be sent at any time. After it has been enabled, standard IPMI commands for setting channel configuration that specify a LAN channel other than the first will return an error code.

### 6.11.3.5    BMC IP Address Configuration

Enabling the BMC's network interfaces requires using the *Set LAN Configuration Parameter* command to configure LAN configuration parameter 4, *IP Address Source*. The BMC supports this parameter as follows:

- 1h, static address (manually configured): Supported on all management NICs. This is the BMC's default value.

- 2h, address obtained by BMC running DHCP: Supported only on embedded management NICs.

IP Address Source value 4h, address obtained by BMC running other address assignment protocol, is not supported on any management NIC.

Attempting to set an unsupported IP address source value has no effect, and the BMC returns error code 0xCC, Invalid data field-in request. Note that values 0h and 3h are no longer supported, and will return a 0xCC error completion code.

### 6.11.3.5.1    Static IP Address (IP Address Source Values 0h, 1h, and 3h)

The BMC supports static IP address assignment on all of its management NICs. The IP address source parameter must be set to *static* before the IP address; the subnet mask or gateway address can be manually set.

The BMC takes no special action when the following IP address source is specified as the IP address source for any management NIC: 1h – Static address (manually configured).

The *Set LAN Configuration Parameter* command must be used to configure LAN configuration parameter 3, *IP Address*, with an appropriate value.

The BIOS does not monitor the value of this parameter, and it does not execute DHCP for the BMC under any circumstances, regardless of the BMC configuration.

### 6.11.3.5.2    Static LAN Configuration Parameters

When the IP Address Configuration parameter is set to 01h (static), the following parameters may be changed by the user:

- LAN configuration parameter 3 (IP Address)
- LAN configuration parameter 6 (Subnet Mask)
- LAN configuration parameter 12 (Default Gateway Address)

When changing from DHCP to Static configuration, the initial values of these three parameters will be equivalent to the existing DHCP-set parameters. Additionally, the BMC observes the following network safety precautions:

1. The user may only set a subnet mask that is valid, per IPv4 and RFC 950 (*Internet Standard Subnetting Procedure*). Invalid subnet values return a 0xCC (Invalid Data Field in Request) completion code, and the subnet mask is not set. If no valid mask has been previously set, default subnet mask is 0.0.0.0.

2. The user may only set a default gateway address that can potentially exist within the subnet specified above. Default gateway addresses outside the BMC's subnet are technically unreachable and the BMC will not set the default gateway address to an unreachable value. The BMC returns a 0xCC (Invalid Data Field in Request) completion code for default gateway addresses outside its subnet.

3. If a command is issued to set the default gateway IP address before the BMC's IP address and subnet mask are set, the default gateway IP address is not updated and the BMC returns 0xCC.

If the BMC's IP address on a LAN channel changes while a LAN session is in progress over that channel, the BMC does not take action to close the session except through a normal session timeout. The remote

client must re-sync with the new IP address. The BMC's new IP address is only available in-band through the *Get LAN Configuration Parameters* command.

### 6.11.3.5.3   Enabling/Disabling Dynamic Host Configuration (DHCP) Protocol

The BMC DHCP feature is activated by using the *Set LAN Configuration Parameter* command to set LAN configuration parameter 4, *IP Address Source*, to 2h: "address obtained by BMC running DHCP". Once this parameter is set, the BMC initiates the DHCP process within approximately 100 ms.

If the BMC has previously been assigned an IP address through DHCP or the *Set LAN Configuration Parameter* command, it requests that same IP address to be reassigned. If the BMC does not receive the same IP address, system management software must be reconfigured to use the new IP address. The new address is only available in-band, through the IPMI *Get LAN Configuration Parameters* command.

Changing the *IP Address Source* parameter from 2h to any other supported value will cause the BMC to stop the DHCP process. The BMC uses the most recently obtained IP address until it is reconfigured.

If the physical LAN connection is lost (that is, the cable is unplugged), the BMC will not re-initiate the DHCP process when the connection is re-established.

### 6.11.3.5.4   DHCP-related LAN Configuration Parameters

Users may not change the following LAN parameters while the DHCP is enabled:

- LAN configuration parameter 3 (IP Address)
- LAN configuration parameter 6 (Subnet Mask)
- LAN configuration parameter 12 (Default Gateway Address)

To prevent users from disrupting the BMC's LAN configuration, the BMC treats these parameters as read-only while DHCP is enabled for the associated LAN channel. Using the *Set LAN Configuration Parameter* command to attempt to change one of these parameters under such circumstances has no effect, and the BMC returns error code 0xD5, "Cannot Execute Command. Command, or request parameter(s) are not supported in present state."

### 6.11.3.6      DHCP BMC Hostname

The BMC allows setting a DHCP Hostname using the *Set/Get LAN Configuration Parameters* command.

- DHCP Hostname can be set regardless of the IP Address source configured on the BMC. But this parameter is only used if the IP Address source is set to DHCP.
- When Byte 2 is set to *Update in progress*, all the 16 Block Data Bytes (Bytes 3 – 18) must be present in the request.
- When Block Size is less than 16, it must be the last Block request in this series. In other words Byte 2 is equal to "*Update is complete*" on that request.
- Whenever Block Size is less than 16, the Block data bytes must end with a NULL Character or Byte (=0).
- All Block write requests are updated into a local Memory byte array. When Byte 2 is set to *Update is Complete*, the Local Memory is committed to the NV Storage. Local Memory is reset to NULL after changes are committed.

- When Byte 1 (Block Selector = 1), firmware resets all the 64 bytes local memory. This can be used to undo any changes after the last *Update in Progress*.

- User should always set the hostname starting from block selector 1 after the last *Update is complete*. If the user skips block selector 1 while setting the hostname, the BMC will record the hostname as *NULL*, because the first block contains NULL data.

- This scheme effectively does not allow a user to make a partial Hostname change. Any Hostname change needs to start from Block 1.

- Byte 64 ( Block Selector 04h byte 16) is always ignored and set to NULL by BMC which effectively means we can set only 63 bytes.

- User is responsible for keeping track of the Set series of commands and Local Memory contents.

While BMC firmware is in *Set Hostname in Progress* (Update not complete), the firmware continues using the Previous Hostname for DHCP purposes.

## 6.11.4    Address Resolution Protocol (ARP)

The BMC can receive and respond to ARP requests on BMC NICs. Gratuitous ARPs are supported, and disabled by default.

## 6.11.5    Internet Control Message Protocol (ICMP)

The BMC supports the following ICMP message types targeting the BMC over integrated NICs:

- Echo request (ping): The BMC sends an Echo Reply.

- Destination unreachable: If message is associated with an active socket connection within the BMC, the BMC closes the socket.

## 6.11.6    Virtual Local Area Network (VLAN)

The BMC supports VLAN as defined by IPMI 2.0 specifications. VLAN is supported internally by the BMC, not through switches. VLAN provides a way of grouping a set of systems together so that they form a logical network. This feature can be used to set up a management VLAN where only devices which are members of the VLAN will receive packets related to management and members of the VLAN will be isolated from any other network traffic. Note that VLAN does not change the behavior of the host network setting, and it only affects the BMC LAN communication.

LAN configuration options are now supported (by means of the *Set LAN Config Parameters* command, parameters 20 and 21) that allow support for 802.1Q VLAN (Layer 2). This allows VLAN headers/packets to be used for IPMI LAN sessions. VLAN IDs are entered and enabled by means of parameter 20 of the *Set LAN Config Parameters* IPMI command. When a VLAN ID is configured and enabled, the BMC only accepts packets with that VLAN tag/ID. Conversely, all BMC generated LAN packets on the channel include the given VLAN tag/ID. Valid VLAN IDs are 1 through 4094, and VLAN IDs of 0 and 4095 are reserved, per the 802.1Q VLAN specification.

Parameter 21 (VLAN Priority) of the *Set LAN Config Parameters* IPMI command is now implemented and a range from 0 to 7 will be allowed for VLAN Priorities. Note that bits 3 and 4 of Parameter 21 are considered Reserved bits.

Parameter 25 (VLAN Destination Address) of the *Set LAN Config Parameters* IPMI command is not supported and returns a completion code of 0x80 (parameter not supported) for any read/write of parameter 25.

If the BMC IP address source is DHCP, the following behavior is seen:

- If the BMC is first configured for DHCP (prior to enabling VLAN), when VLAN is enabled, the BMC performs a discovery on the new VLAN in order to obtain a new BMC IP address.
- If the BMC is configured for DHCP (before disabling VLAN), when VLAN is disabled, the BMC performs a discovery on the LAN in order to obtain a new BMC IP address.

If the BMC IP address source is Static, the following behavior is seen:

- If the BMC is first configured for static (prior to enabling VLAN), when VLAN is enabled, the BMC has the same IP address as configured before. It is left to the management application to configure a different IP address if that is not suitable for VLAN.
- If the BMC is configure for static (prior to disabling VLAN), when VLAN is disabled, the BMC has the same IP address as configured before. It is left to the management application to configure a different IP address if that is not suitable for LAN.

### 6.11.7    Secure Shell (SSH)

Secure Shell (SSH) connections are supported for SMASH-CLP sessions to the BMC.

There is a maximum of one SMASH-CLP session allowed.

### 6.11.8    Serial-over-LAN (SOL 2.0)

The BMC supports IPMI 2.0 SOL.

IPMI 2.0 introduced a standard serial-over-LAN feature. This is implemented as a standard payload type (01h) over RMCP+.

Three commands are implemented for SOL 2.0 configuration:

- Get SOL 2.0 Configuration Parameters and Set SOL 2.0 Configuration Parameters: These commands are used to get and set the values of the SOL configuration parameters. The parameters are implemented on a per-channel basis.
- Activating SOL: This command is not accepted by the BMC. It is sent by the BMC when SOL is activated to notify a remote client of the switch to SOL.
- Activating a SOL session requires an existing IPMI-over-LAN session. If encryption is used, it should be negotiated when the IPMI-over LAN session is established.

### 6.11.9    Platform Event Filter (PEF)

The BMC includes the ability to generate a selectable action, such as a system power-off or reset, when a match occurs to one of a configurable set of events. This capability is called *Platform Event Filtering*, or PEF. One of the available PEF actions is to trigger the BMC to send a LAN alert to one or more destinations.

The BMC supports 20 PEF filters. The first twelve entries in the PEF filter table are pre-configured (but may be changed by the user). The remaining entries are left blank, and may be configured by the user.

**Table 16. Factory Configured PEF Table Entries**

| Event Filter Number | Offset Mask | Events |
|---|---|---|
| 1 | Non-critical, critical and non-recoverable | Temperature sensor out of range |
| 2 | Non-critical, critical and non-recoverable | Voltage sensor out of range |
| 3 | Non-critical, critical and non-recoverable | Fan failure |
| 4 | General chassis intrusion | Chassis intrusion (security violation) |
| 5 | Failure and predictive failure | Power supply failure |
| 6 | Uncorrectable ECC | BIOS |
| 7 | POST error | BIOS: POST code error |
| 8 | FRB2 | Watchdog Timer expiration for FRB2 |
| 9 | Policy Correction Time | Node Manager |
| 10 | Power down, power cycle, and reset | Watchdog timer |
| 11 | OEM system boot event | System restart (reboot) |
| 12 | Drive Failure, Predicted Failure | Hot Swap Controller |

Additionally, the BMC supports the following PEF actions:

- Power off
- Power cycle
- Reset
- OEM action
- Alerts

The *Diagnostic interrupt* action is not supported.

## 6.11.10    LAN Alerting

The BMC supports sending embedded LAN alerts, called SNMP PET (Platform Event traps), and SMTP email alerts.

The BMC supports a minimum of four LAN alert destinations.

### 6.11.10.1      SNMP Platform Event Traps (PETs)

This feature enables a target system to send SNMP traps to a designated IP address by means of LAN. These alerts are formatted per the *Intelligent Platform Management Interface Specification Second Generation v2.0*. A Modular Information Block (MIB) file associated with the traps is provided with the BMC firmware to facilitate interpretation of the traps by external software. The format of the MIB file is covered under RFC 2578.

## 6.11.11    Alert Policy Table

Associated with each PEF entry is an alert policy that determines which IPMI channel the alert is to be sent. There is a maximum of 20 alert policy entries. There are no pre-configured entries in the alert policy table because the destination types and alerts may vary by user. Each entry in the alert policy table contains four bytes for a maximum table size of 80 bytes.

### 6.11.11.1       E-mail Alerting

The Embedded Email Alerting feature allows the user to receive e-mails alerts indicating issues with the server. This allows e-mail alerting in an OS-absent (for example, Pre-OS and OS-Hung) situation. This feature provides support for sending e-mail by means of SMTP, the Simple Mail Transport Protocol as defined in Internet RC 821. The e-mail alert provides a text string that describes a simple description of the event. SMTP alerting is configured using the embedded web server.

## 6.11.12    SM-CLP (SM-CLP Lite)

SMASH refers to Systems Management Architecture for Server Hardware. SMASH is defined by a suite of specifications, managed by the DMTF, that standardize the manageability interfaces for server hardware. CLP refers to Command Line Protocol. SM-CLP is defined by the *Server Management Command Line Protocol Specification (SM-CLP) ver1.0*, which is part of the SMASH suite of specifications. The specifications and further information on SMASH can be found at the DMTF website (http://www.dmtf.org/).

The BMC provides an embedded *lite* version of SM-CLP that is syntax-compatible but not considered fully compliant with the DMTF standards.

The SM-CLP utilized by a remote user by connecting a remote system using one of the system NICs. It is possible for third-party management applications to create scripts using this CLP and execute them on server to retrieve information or perform management tasks such as reboot the server, configure events, and so on.

The BMC embedded SM-CLP feature includes the following capabilities:

- Power on/off/reset the server.
- Get the system power state.
- Clear the System Event Log (SEL).
- Get the interpreted SEL in a readable format.
- Initiate/terminate a Serial Over LAN session.
- Support "help" to provide helpful information.
- Get/set the system ID LED.
- Get the system GUID.
- Get/set configuration of user accounts.
- Get/set configuration of LAN parameters.
- Embedded CLP communication should support SSH connection.
- Provide current status of platform sensors including current values. Sensors include voltage, temperature, fans, power supplies, and redundancy (power unit and fan redundancy).

### 6.11.13    Embedded Web Server

The embedded web server is supported over any system NIC port that is enabled for server management capabilities.

BMC Base manageability provides an embedded web server and an OEM-customizable web GUI which exposes the manageability features of the BMC base feature set. It is supported over all on-board NICs that have management connectivity to the BMC as well as an optional RMM4 dedicated add-in management NIC. At least two concurrent web sessions from up to two different users is supported. The embedded web user interface supports the following client web browsers:

- Microsoft Internet Explorer 9.0*
- Microsoft Internet Explorer 10.0*
- Mozilla Firefox 24*
- Mozilla Firefox 25*

The embedded web user interface supports strong security (authentication, encryption, and firewall support) since it enables remote server configuration and control. Embedded web server uses ports #80 and #443. The user interface presented by the embedded web user interface authenticates the user before allowing a web session to be initiated. Encryption using 128-bit SSL is supported. User authentication is based on user ID and password.

The GUI presented by the embedded web server authenticates the user before allowing a web session to be initiated. It presents all functions to all users but grays-out those functions that the user does not have privilege to execute. (For example, if a user does not have privilege to power control, the item will be displayed in grey-out font in that user's UI display). The web GUI also provides a launch point for some of the advanced features, such as KVM and media redirection. These features are grayed out in the GUI unless the system has been updated to support these advanced features. The embedded web server only displays US English or Chinese language output.

Additional features supported by the web GUI includes:

- Present all the Basic features to the users.
- Power on/off/reset the server and view current power state.
- Display BIOS, BMC, ME, and SDR version information.
- Display overall system health.
- Configuration of various IPMI over LAN parameters for both IPV4 and IPV6.
- Configuration of alerting (SNMP and SMTP).
- Display system asset information for the product, board, and chassis.
- Display of BMC-owned sensors (name, status, current reading, enabled thresholds), including color-code status of sensors.
- Provide ability to filter sensors based on sensor type (Voltage, Temperature, Fan, and Power supply related).
- Automatic refresh of sensor data with a configurable refresh rate.
- Online help

- Display/clear SEL (display is in easily understandable human readable format).

- Support major industry-standard browsers (Microsoft Internet Explorer* and Mozilla Firefox*).

- The GUI session automatically times-out after a user-configurable inactivity period. By default, this inactivity period is 30 minutes.

- Embedded Platform Debug feature: Allows the user to initiate a *diagnostic dump* to a file that can be sent to Intel for debug purposes.

- Virtual Front Panel: The Virtual Front Panel provides the same functionality as the local front panel. The displayed LEDs match the current state of the local panel LEDs. The displayed buttons (for example, power button) can be used in the same manner as the local buttons.

- Display of ME sensor data. Only sensors that have associated SDRs loaded are displayed.

- Ability to save the SEL to a file.

- Ability to force HTTPS connectivity for greater security. This is provided through a configuration option in the UI.

- Display of processor and memory information as is available over IPMI over LAN.

- Ability to get and set Node Manager (NM) power policies.

- Display of power consumed by the server.

- Ability to view and configure VLAN settings.

- Warn user the reconfiguration of IP address will cause disconnect.

- Capability to block logins for a period of time after several consecutive failed login attempts. The lock-out period and the number of failed logins that initiates the lock-out period are configurable by the user.

- Server Power Control: Ability to force into Setup on a reset.

- System POST results – The web server provides the system's Power-On Self-Test (POST) sequence for the previous two boot cycles, including timestamps. The timestamps may be viewed in relative to the start of POST or the previous POST code.

- Customizable ports – The web server provides the ability to customize the port numbers used for SMASH, http, https, KVM, secure KVM, remote media, and secure remote media. The ports provided must be unique. If two identical ports are provided, the associated services will not function properly. Some ports are reserved and cannot be assigned to any of these services because they are used internally; these ports are 623, 8080, and 8282.

- Ability to update SDR. Upload new sensor data repository records and configuration files. Enable/disable SDR auto-configuration.

- Display users currently logged in to the BMC.

- Ability to Restore BMC Defaults

- Ability to select the BMC network interfaces to carry SOL data.

- Ability to view and configure KVM settings.

- Ability to generate and download SOL log file

- Ability to view and configure SOL log feature setting

### 6.11.14   Virtual Front Panel

- Virtual Front Panel is the module present as Virtual Front Panel on the left side in the embedded web server when remote Control tab is clicked.

- Main Purpose of the Virtual Front Panel is to provide the front panel functionality virtually.

- Virtual Front Panel (VFP) will mimic the status LED and Power LED status and Chassis ID alone. It is automatically in sync with BMC every 40 seconds.

- For any abnormal status LED state, Virtual Front Panel will get the reason behind the abnormal or status LED changes and displayed in VFP side.

- As Virtual Front Panel uses the *Chassis Control* command for power actions. It won't log the Front button press event since Logging the front panel press event for Virtual Front Panel press will mislead the administrator.

- For Reset from Virtual Front Panel, the reset will be done by a *Chassis Control* command.

- During Power action, Power button/Reset button will not accept the next action until current Power action is complete and the acknowledgment from BMC is received.

- Embeded Web Server (EWS) will provide a valid message during Power action until it completes the current Power action.

- The VFP does not have any effect on whether the front panel is locked by *Set Front Panel Enables* command.

- The chassis ID LED provides a visual indication of a system being serviced. The state of the chassis ID LED is affected by the following actions:

  - Toggled by turning the chassis ID button on or off.

  - There is no precedence or lock-out mechanism for the control sources. When a new request arrives, previous requests are terminated. For example, if the chassis ID button is pressed, the chassis ID LED changes to solid on. If the button is pressed again, the chassis ID LED turns off.

  - Note that the chassis ID will turn on because of the original chassis ID button press and will reflect in the Virtual Front Panel after VFP sync with BMC. Virtual Front Panel will not reflect the chassis LED software blinking from the software command as there is no mechanism to get the chassis ID Led status.

  - Only Infinite chassis ID ON/OFF from the software command will reflect in EWS during automatic /manual EWS sync up with BMC.

- Virtual Front Panel help is available for virtual panel module.

- At present, NMI button in VFP is disabled. It can be used in future.

## 6.11.15    Embedded Platform Debug

The Embedded Platform Debug feature supports capturing low-level diagnostic data (applicable MSRs, PCI config-space registers, and so on). This feature allows a user to export this data into a file that is retrievable from the embedded web GUI, as well as through host and remote IPMI methods, for the purpose of sending to an Intel engineer for an enhanced debugging capability. The files are compressed, encrypted, and password protected. The file is not meant to be viewable by the end user but rather to provide additional debugging capability to an Intel support engineer.

A list of data that may be captured using this feature includes but is not limited to:

- Platform sensor readings – This includes all readable sensors that can be accessed by the BMC FW and have associated SDRs populated in the SDR repository. This does not include any event-only sensors. (All BIOS sensors and some BMC and ME sensors are event-only; meaning that they

are not readable using an IPMI *Get Sensor Reading* command but rather are used just for event logging purposes).

- SEL – The current SEL contents are saved in both hexadecimal and text format.

- CPU/memory register data – Useful for diagnosing the cause of the following system errors: CATERR, ERR[2], SMI timeout, PERR, and SERR. The debug data is saved and time stamped for the last 3 occurrences of the error conditions.

  - First 256 byte of PCI configuration space and the advanced error reporting registers
  - Processor Machine Check Architecture registers
  - Integrated Memory Controller (iMC) Machine Check Architecture registers
  - Integrated I/O (IIO) Global error registers

- BMC configuration data

  - BMC FW debug log (that is, SysLog) – Captures FW debug messages.
  - Non-volatile storage of captured data – Some of the captured data is stored persistently in the BMC's non-volatile flash memory and preserved across AC power cycles. Due to size limitations of the BMC's flash memory, it is not feasible to store all of the data persistently.

- SMBIOS table data – The entire SMBIOS table is captured from the last boot.

- PCI configuration data for on-board devices and add-in cards – The first 256 bytes of PCI configuration data is captured for each device for each boot.

- Power supplies debug capability

  - Capture of power supply *black box* data and power supply asset information – Power supply vendors are adding the capability to store debug data within the power supply itself. The platform debug feature provides a means to capture this data for each installed power supply. The data can be analyzed by Intel® for failure analysis and possibly provided to the power supply vendor as well. The BMC gets this data from the power supplied from the PMBus* manufacturer-specific commands.
  - Storage of system identification in power supply – The BMC copies board and system serial numbers and part numbers into the power supply whenever a new power supply is installed in the system or when the system is first powered on. This information is included as part of the power supply black box data for each installed power supply.

- Accessibility through IPMI interfaces – The platform debug file can be accessed using an external IPMI interface (KCS or LAN).

- POST code sequence for the two most recent boots – This is a best-effort data collection by the BMC as the BMC real-time response cannot guarantee that all POST codes are captured.

  - SDR data.
  - Signal debugging dumps, if available.

- Support for multiple debug files –The platform debug feature provides the ability to save data to two separate files that are encrypted with different passwords.

- File #1 is strictly for viewing by Intel engineering and may contain BMC log messages (that is, syslog) and other debug data that Intel FW developers deem useful in addition to the data specified in this document.
- File #2 can be viewed by Intel partners who have signed an NDA with Intel and its contents are restricted to specific data items specified in this with the exception of the BMC syslog messages and power supply *black box* data.

### 6.11.15.1    Output Data Format

The diagnostic feature outputs a password-protected compressed HTML file containing specific BMC and system information. This file is not intended for end-customer usage. This file is for customer support and engineering only.

### 6.11.15.2    Output Data Availability

The diagnostic data is available on-demand from the embedded web server, KCS, or IPMI *Over LAN* commands.

### 6.11.15.3    Output Data Categories

The following tables list the data to be provided in the diagnostic output. For items in Table 17, this data is collected on detection of CATERR, ERR2, PERR, SERR, and SMI timeout. The data in Table 18 is accumulated for the three most recent overall errors.

**Table 17. Diagnostic Data**

| Category | Data |
|---|---|
| Internal BMC Data | BMC uptime/load |
| | Process list |
| | Free Memory |
| | Detailed Memory List |
| | Filesystem List/Info |
| | BMC Network Info |
| | BMC Syslog |
| | BMC Configuration Data |
| External BMC Data | Sensor readings |
| | Hex SEL listing |
| | Human-readable SEL listing |
| | Human-readable sensor listing |
| External BIOS Data | POST codes for the two most recent boots |
| System Data | SMBIOS table for the current boot |
| | Power Supply Unit data |

**Table 18. Additional Diagnostics on Error**

| Category | Data |
|---|---|
| System Data | First 256 bytes of PCI config data for each PCI device |

| Category | Data |
|---|---|
| | PCI advanced error reporting registers |
| | Processor Machine Check Architecure registers |
| | iMC Machine Check Architecure registers |
| | IIO Global error registers |

## 6.11.16    Data Center Management Interface (DCMI)

The *DCMI Specification* is an emerging standard that is targeted to provide a simplified management interface for Internet Portal Data Center (IPDC) customers. It is expected to become a requirement for server platforms which are targeted for IPDCs. DCMI is an IPMI-based standard that builds upon a set of required IPMI standard commands by adding a set of DCMI-specific IPMI OEM commands. Intel® S1200SP Server Platforms implement the mandatory DCMI features in the BMC firmware (DCMI 1.5 compliance). Refer to *DCMI 1.5 spec* for details. Only mandatory commands are supported. No support for optional DCMI commands. Optional power management and SEL roll over feature is not supported. DCMI Asset tag is independent of baseboard FRU asset Tag.

## 6.11.17    Lightweight Directory Access Protocol (LDAP)

The Lightweight Directory Access Protocol (LDAP) is an application protocol supported by the BMC for the purpose of authentication and authorization. The BMC user connects with an LDAP server for login authentication. This is only supported for non-IPMI logins including the embedded web UI and SM-CLP. IPMI users/passwords and sessions are not supported over LDAP. LDAP can be configured (IP address of LDAP server, port, and so on) using the BMC's Embedded Web UI. LDAP authentication and authorization is supported over the any NIC configured for system management. The BMC uses a standard Open LDAP implementation for Linux*. Only open LDAP is supported by BMC. Microsoft Windows* and Novell* LDAP are not supported.

# 7.    Advanced Management Feature Support (RMM4)

The integrated BMC has support for basic and advanced server management features. Basic management features are available by default. Advanced management features are enabled with the addition of an optionally installed Remote Management Module 4 Lite (RMM4 Lite) key.

**Table 19. Intel® Remote Management Module 4 (RMM4) Options**

| Intel Product Code | Description | Kit Contents | Benefits |
|---|---|---|---|
| AXXRMM4LITE | Intel® Remote Management Module 4 Lite | RMM4 Lite Activation Key | Enables KVM & media redirection |

When the BMC FW initializes, it attempts to access the Intel® RMM4 Lite. If the attempt to access the Intel® RMM4 Lite is successful, then the BMC activates the advanced features.
On the server board Intel® RMM4 Lite key is installed at the following locations.
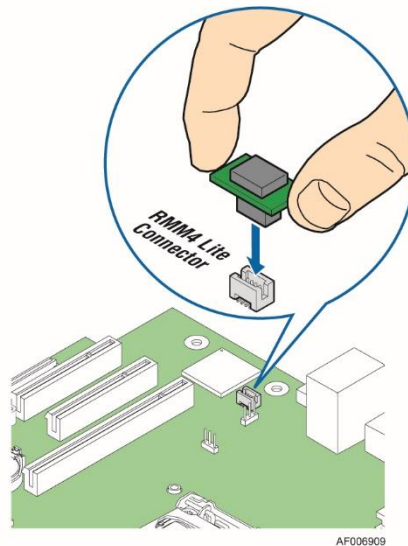


**Figure 18. Intel® RMM4 Lite Activation Key Installation**

## 7.1    Dedicated Management Port

The Intel® server board S1200SPL includes a dedicated 1GbE RJ45 Management Port. The management port is active with or without the RMM4 Lite key installed.

## 7.2    Keyboard, Video, and Mouse (KVM) Redirection

The BMC firmware supports keyboard, video, and mouse redirection (KVM) over LAN. This feature is available remotely from the embedded web server as a Java applet. This feature is only enabled when the Intel® RMM4 lite is present. The client system must have a Java Runtime Environment* (JRE*) version 6.0 or later to run the KVM or media redirection applets.

The BMC supports an embedded KVM application (Remote Console) that can be launched from the embedded web server from a remote console. USB1.1 or USB 2.0 based mouse and keyboard redirection are supported. It is also possible to use the KVM-redirection (KVM-r) session concurrently with media-redirection (media-r). This feature allows a user to interactively use the keyboard, video, and mouse functions of the remote server as if the user were physically at the managed server.

KVM redirection console supports the following keyboard layouts: English, Dutch, French, German, Italian, Russian, and Spanish.

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.

Other attributes of this feature include:

- Encryption of the redirected screen, keyboard, and mouse
- Compression of the redirected screen
- Ability to select a mouse configuration based on the OS type
- Supports user definable keyboard macros

KVM redirection feature supports the following resolutions and refresh rates:

- 640x480 at 60Hz, 72Hz, 75Hz, 85Hz, 100Hz
- 800x600 at 60Hz, 72Hz, 75Hz, 85Hz
- 1024x768 at 60Hz, 72Hz, 75Hz, 85Hz
- 1280x960 at 60Hz
- 1280x1024 at 60Hz
- 1600x1200 at 60Hz
- 1920x1080 (1080p),
- 1920x1200 (WUXGA)
- 1650x1080 (WSXGA+)

## 7.2.1 Remote Console

The Remote Console is the redirected screen, keyboard and mouse of the remote host system. To use the Remote Console window of your managed host system, the browser must include a Java* Runtime Environment plug-in. If the browser has no Java support, such as with a small handheld device, the user can maintain the remote host system using the administration forms displayed by the browser.

The Remote Console window is a Java Applet that establishes TCP connections to the BMC. The protocol that is run over these connections is a unique KVM protocol and not HTTP or HTTPS. This protocol uses ports #7578 for KVM, #5120 for CDROM media redirection, and #5123 for Floppy/USB media redirection. When encryption is enabled, the protocol uses ports #7582 for KVM, #5124 for CDROM media redirection,

and #5127 for Floppy/USB media redirection. The local network environment must permit these connections to be made, that is, the firewall and, in case of a private internal network, the NAT (Network Address Translation) settings have to be configured accordingly.

### 7.2.2 Performance

The remote display accurately represents the local display. The feature adapts to changes to the video resolution of the local display and continues to work smoothly when the system transitions from graphics to text or vice versa. The responsiveness may be slightly delayed depending on the bandwidth and latency of the network.

Enabling KVM and/or media encryption will degrade performance. Enabling video compression provides the fastest response while disabling compression provides better video quality.

For the best possible KVM performance, a 2Mb/sec link or higher is recommended.

The redirection of KVM over IP is performed in parallel with the local KVM without affecting the local KVM operation.

### 7.2.3 Security

The KVM redirection feature supports multiple encryption algorithms, including RC4 and AES. The actual algorithm that is used is negotiated with the client based on the client's capabilities.

### 7.2.4 Availability

The remote KVM session is available even when the server is powered-off (in stand-by mode). No re-start of the remote KVM session is required during a server reset or power on/off. A BMC reset (for example, due to a BMC Watchdog initiated reset or BMC reset after BMC FW update) requires the session to be re-established.

KVM sessions persist across system reset, but not across an AC power loss.

### 7.2.5 Usage

As the server is powered up, the remote KVM session displays the complete BIOS boot process. The user can interact with BIOS setup, change and save settings as well as enter and interact with option ROM configuration screens.

At least two concurrent remote KVM sessions are supported. It is possible for at least two different users to connect to the same server and start remote KVM sessions.

### 7.2.6 Force-enter BIOS Setup

KVM redirection can present an option to force-enter BIOS Setup. This enables the system to enter F2 setup while booting which is often missed by the time the remote console redirects the video.

## 7.3 Media Redirection

The embedded web server provides a Java applet to enable remote media redirection. This may be used in conjunction with the remote KVM feature, or as a standalone applet.

The media redirection feature is intended to allow system administrators or users to mount a remote IDE or USB CD-ROM, floppy drive, or a USB flash disk as a remote device to the server. Once mounted, the remote device appears just like a local device to the server, allowing system administrators or users to install software (including operating systems), copy files, update BIOS, and so on, or boot the server from this device.

The following capabilities are supported:

- The operation of remotely mounted devices is independent of the local devices on the server. Both remote and local devices are useable in parallel.
- Either IDE (CD-ROM, floppy) or USB devices can be mounted as a remote device to the server.
- It is possible to boot all supported operating systems from the remotely mounted device and to boot from disk IMAGE (*.IMG) and CD-ROM or DVD-ROM ISO files. See the Tested/supported Operating System List for more information.
- Media redirection supports redirection for both a virtual CD device and a virtual Floppy/USB device concurrently. The CD device may be either a local CD drive or else an ISO image file; the Floppy/USB device may be a local Floppy drive, a local USB device, or a disk image file.
- The media redirection feature supports multiple encryption algorithms, including RC4 and AES. The actual algorithm that is used is negotiated with the client based on the client's capabilities.
- A remote media session is maintained even when the server is powered-off (in standby mode). No restart of the remote media session is required during a server reset or power on/off. A BMC reset (for example, due to a BMC reset after BMC FW update) requires the session to be re-established
- The mounted device is visible to (and useable by) managed system's OS and BIOS in both pre-boot and post-boot states.
- The mounted device shows up in the BIOS boot order and it is possible to change the BIOS boot order to boot from this remote device.
- It is possible to install an operating system on a bare metal server (no OS present) using the remotely mounted device. This may also require the use of KVM-r to configure the OS during install.

USB storage devices appear as floppy disks over media redirection. This allows for the installation of device drivers during OS installation.

If either a virtual IDE or virtual floppy device is remotely attached during system boot, both the virtual IDE and virtual floppy are presented as bootable devices. It is not possible to present only a single-mounted device type to the system BIOS.

## 7.3.1    Availability

The default inactivity timeout is 30 minutes and is not user-configurable. Media redirection sessions persist across system reset but not across an AC power loss or BMC reset.

## 7.3.2    Network Port Usage

The KVM and media redirection features use the following ports:

- 5120 – CD Redirection

- 5123 – FD Redirection
- 5124 – CD Redirection (Secure)
- 5127 – FD Redirection (Secure)
- 7578 – Video Redirection
- 7582 – Video Redirection (Secure)

# 8.    On-board Connector/Header Overview

The following section provides detailed information regarding all connectors, headers, and jumpers on the server boards.

## 8.1    Board Connector Information

The following table lists all connector types available on the board and the corresponding preference designators printed on the silkscreen.

**Table 20. Board Connector Matrix**

| Connector | Quantity | Reference Designators | Connector Type | Pin Count |
|---|---|---|---|---|
| Power supply | 3 | J9H1<br>J9B1<br>J9F1 | Main power<br>CPU power<br>PS AUX | 24<br>8<br>5 |
| CPU | 1 | U6F1 | CPU sockets | 1151 |
| Main memory | 4 | J7C1, J8C2, J8C3, J9C1 | DIMM sockets | 240 |
| PCI Express* x8 mechanical | 2 | J1B1, J2B1 | Card edge | 98 |
| PCI Express* x16 mechanical | 1 | J3B2 | Card edge | 164 |
| RJ45+USB 3.0 connector | 1 | JA5A1 | Connector | 32 |
| NIC connector | 2 | JA7A1, J6A2 | Connector | |
| Intel® RMM4 Lite | 1 | J3B1 | Connector | 8 |
| SATA Key to enable ESRT2 RAID5 | 1 | J9K1 | Header | 4 |
| System fans | 4 | J3K2, J8K2, J8K3, J8B1 | Header | 4 |
| CPU fan | 1 | J7K1 | Header | 4 |
| Battery | 1 | BT2F1 | Battery holder | 2 |
| VGA | 1 | J8A1 | Connector | 15 |
| Display Port | 1 | J4A1 | Connector | 4 |
| Serial port | 1 | J9A1 | Connector | 9 |
| Front panel | 1 | J9E1 | Header | 24 |
| USB 2.0 rear IO | 1 | J6A1 | connector | 8 |
| Internal Dual USB 3.0 | 1 | J1J1 | Header | 20 |
| Internal Dual USB 2.0 | 1 | J1J2 | Header | 10 |
| M.2 SSD | 1 | J2G1 | connector | 75 |
| Internal USB | 1 | J1K3 | Type-A USB | 4 |
| SATA | 8 | J1K4, J1K1, J1K5,<br>J1K2, J2K4, J2K3, J2K1, J2K2 | Connector | 7 |

| Connector | Quantity | Reference Designators | Connector Type | Pin Count |
|---|---|---|---|---|
| HSBP_I2C | 1 | J3K3 | Header | 3 |
| SATA SGPIO | 2 | J2K5, J2K6 | Header | 5 |
| LCP (Header reserved but LCP module not supported) | 1 | J1G3 | Header | 7 |
| IPMB | 1 | J1G2 | Header | 4 |
| Configuration jumpers | 5 | J4B1 (Force Integrated BMC update), J1F4 (Password Clear), J7B1 (BIOS Recovery), J4C1 (Reset BIOS Configuration) J1F1 (ME Firmware Update) | Jumper | 3 |
| TPM | 1 | J8K1 | Connector | 14 |
| Chassis Intrusion | 1 | J9B2 | Header | 2 |
| I/O Module Connector | 1 | J1C1 | Connector | 80 |
| SAS Module Connector | 1 | J4J1 | Connector | 80 |

## 8.2    Power Connectors

The main power supply connection uses an SSI-compliant 2x12 pin connector (J9H1).

Two additional power-related connectors also exist:

- One SSI-compliant 2x4 pin power connector (J9B1) to provide 12-V power to the CPU voltage regulators and memory.
- One SSI-compliant 1x5 pin connector (J9F1) to provide I2C monitoring of the power supply.

The following tables define these connector pin-outs:

**Table 21. Main Power Connector Pin–out (J9H1)**

| Pin | IO | Signal Name | Pin | IO | Signal Name |
|---|---|---|---|---|---|
| 1 | PWR | +3.3V | 13 | PWR | +3.3V |
| 2 | PWR | +3.3V | 14 | PWR | -12V (NA for most designs) |
| 3 | GND | GND | 15 | GND | GND |
| 4 | PWR | +5V | 16 | I | PS_ON# |
| 5 | GND | GND | 17 | GND | GND |
| 6 | PWR | +5V | 18 | GND | GND |
| 7 | GND | GND | 19 | GND | GND |
| 8 | O | PWR_GD | 20 | NC | NC |
| 9 | PWR | SB5V | 21 | PWR | +5V |
| 10 | PWR | +12V | 22 | PWR | +5V |
| 11 | PWR | +12V | 23 | PWR | +5V |
| 12 | PWR | +3.3V | 24 | GND | GND |

**Table 22. CPU Power Connector Pin–out (J9B1)**

| Pin | IO | Signal Name | Pin | IO | Signal Name |
|---|---|---|---|---|---|
| 1 | GND | GND | 5 | PWR | P12V1 |
| 2 | GND | GND | 6 | PWR | P12V1 |
| 3 | GND | GND | 7 | PWR | P12V2 |
| 4 | GND | GND | 8 | PWR | P12V2 |

**Table 23. PMBUS SSI Connector Pin-out (J9F1)**

| Pin | IO | Signal Name |
|---|---|---|
| 1 | I | PMBUS_CLK |
| 2 | IO | PMBUS_DATA |
| 3 | O | IRQ_PMBUS_ALERT_N |
| 4 | GND | GND Return Sense |
| 5 | I | P3V3 Sense |

**Table 24. Battery Holder (BT2F1)**

| Pin | IO | Signal Name |
|---|---|---|
| 1 | PWR | P3V_BAT |
| 2 | GND | GND |

## 8.3    System Management Headers

### 8.3.1    Intel® Remote Management Module 4 Lite Connector

The S1200SPL server board provides a 7-pin Intel® RMM4 Lite connector and a stacked connector that includes a USB 3.0 and a dedicated 1GbE RJ45 Management Port. The management port is active with or without the RMM4 Lite key installed. The S1200SPS board does not support Intel® RMM4.

This server board does not support third-party management cards.

*Note: This connector is not compatible with the previous generation Intel® Remote Management Modules (Intel® RMM/RMM2/RMM3)*

**Table 25. Stacked connector of USB 3.0+ dedicated RJ45 Management Port Pin-out (JA5A1)**

| Pin | IO | Name | Pin | IO | Name |
|---|---|---|---|---|---|
| 1 | PWR | P5V_AUX | 17 | I | USB3_TX_DN |
| 2 | IO | USB2_DN | 18 | I | USB3_TX_DP |
| 3 | IO | USB2_DP | 19 | PWR | VCT |
| 4 | GND | GND | 20 | IO | MDI_P0 |
| 5 | O | USB3_RX_DN | 21 | IO | MDI_N0 |
| 6 | O | USB3_RX_DP | 22 | IO | MDI_P1 |
| 7 | GND | GND | 23 | IO | MDI_N1 |
| 8 | I | USB3_TX_DN | 24 | IO | MDI_P2 |
| 9 | I | USB3_TX_DP | 25 | IO | MDI_N2 |
| 10 | PWR | P5V_AUX | 26 | IO | MDI_P3 |
| 11 | IO | USB2_DN | 27 | IO | MDI_N3 |
| 12 | IO | USB2_DP | 28 | GND | GND |

| Pin | IO | Name | Pin | IO | Name |
|-----|----|------|-----|----|------|
| 13 | GND | GND | 29 | I | LED1_ANODE |
| 14 | O | USB3_RX_DN | 30 | O | LED1_CATHODE |
| 15 | O | USB3_RX_DP | 31 | IO | LED2_ANODE |
| 16 | GND | GND | 32 | IO | LED2_CATHODE |

**Table 26. Intel® RMM4 – Lite Connector Pin-out (J3B1)**

| Pin | IO | Signal Name | Pin | IO | Signal Name |
|-----|----|-------------|-----|----|-------------|
| 1 | PWR | P3V3_AUX | 2 | O | SPI_RMM4_LITE_DI |
| 3 | NC | NC | 4 | I | SPI_RMM4_LITE_CLK |
| 5 | I | SPI_RMM4_LITE_DO | 6 | GND | GND |
| 7 | I | SPI_RMM4_LITE_CS_N | 8 | GND | GND |

### 8.3.2 TPM Connector

The S1200SPL server board supports TPM 1.2 module. The S1200SPS server board does not support TPM 1.2 module.

**Table 27. TPM Connector Pin-out (J8K1)**

| Pin | IO | Signal Name | Pin | IO | Signal Name |
|-----|----|-------------|-----|----|-------------|
| 1 | NC | Key Pin | 2 | IO | LPC_LAD<1> |
| 3 | IO | LPC_LAD<0> | 4 | GND | GND |
| 5 | IO | IRQ_SERIAL | 6 | I | LPC_FRAME_N |
| 7 | PWR | P3V3 | 8 | GND | GND |
| 9 | I | RST_BMC_NIC_LRESET_LVC3_R_N | 10 | I | CLK_33M_TPM_CONN |
| 11 | IO | LPC_LAD<3> | 12 | GND | GND |
| 13 | GND | GND | 14 | IO | LPC_LAD<2> |

### 8.3.3 Intel® ESRT2 RAID Upgrade Key Connector

The server board provides one connector to support Intel® ESRT2 RAID Upgrade Key. The I Upgrade Key is a small PCB board that enables RAID 5 software stack of ESRT2 SW RAID. The pin configuration of connector is identical and defined in the following table:

**Table 28. Intel® ESRT2 RAID Upgrade Key Connector Pin-out (J9K1)**

| Pin | IO | Signal Name |
|-----|----|-------------|
| 1 | GND | GND |
| 2 | I | Pull-up (to P3V3_AUX) |
| 3 | GND | GND |
| 4 | I | OW_PCH_SATA_RAID_KEY |

*Note: The ESRT2 RAID 5 under legacy BIOS mode IS NOT supported.*

### 8.3.4 HSBP SMBUS Header

**Table 29. HSBP SMBUS Header Pin-out (J3K3)**

| Pin | IO | Signal Name |
|-----|-----|-------------|
| 1 | IO | SMB_HSBP_DATA |
| 2 | GND | GND |
| 3 | I | SMB_HSBP_CLK |

## 8.3.5     Chassis Intrusion Header

The Chassis Intrusion header is connected via a two-wire cable to a switch assembly that is mounted just under the chassis cover on systems that support this feature. When the chassis cover is removed, the switch and thus the electrical connection between the pins on this header become open allowing the BMC's CHASIS_N pin to be pulled LOW. The BMC's CHASIS-N pin is used by FW to note the change in the chassis cover status.

**Table 30. Chassis Intrusion Header Pin-out (J9B2)**

| Header State | Description |
|--------------|-------------|
| Pins 1 and 2 closed | BMC CHASIS_N is pulled HIGH. Chassis cover is closed. |
| Pins 1 and 2 open | BMC CHASIS_N is pulled LOW. Chassis cover is removed. |

## 8.3.6     SATA SGPIO Header

Two SATA SGPIO 5 pin headers are implemented on board S1200SPL: one is for Port0-3 (White) and the other is for Port4-7 (Black).

**Table 31. SATA SGPIO Header Pin-out (J2K5, J2K6)**

| Pin | IO | Signal Name |
|-----|-----|-------------|
| 1 | I | SGPIO_CLOCK |
| 2 | I | SGPIO_LOAD |
| 3 | GND | GND |
| 4 | I | SGPIO_DATAOUT |
| 5 | O | SGPIO_DATAIN |

## 8.3.7     IPMB Connector

An IPMB header is provided on the baseboard to support connectivity with other IPMI-compliant controllers (e.g. 3rd party management PCIe* cards).

**Table 32. IPMB Connector Pin-out (J1G2)**

| Pin | IO | Signal Name |
|-----|-----|-------------|
| 1 | IO | SMB_IPMB_5VSTBY_DATA |
| 2 | GND | GND |
| 3 | I | SMB_IPMB_5VSTBY_CLK |
| 4 | PWR | P5V_AUX |

## 8.4   Front Panel Connector

The server board provides a 24-pin front panel connector for use with Intel® and third-party chassis. The connector consists of a 24-pin SSI compatible front panel connector. The 24-pin SSI front panel connector provides various front panel features including:

- Power/Sleep Button
- System ID Button

- NMI Button
- NIC Activity LEDs
- Hard Drive Activity LEDs
- System Status LED
- System ID LED

The following table provides the pin-out for this connector:

**Table 33. Front Panel 24-pin Connector Pin-out (J9E1)**

| Pin | IO | Signal Name | Pin | IO | Signal Name |
|-----|-----|-----|-----|-----|-----|
| 1 | PWR | 3VSB (Power LED Anode) | 2 | PWR | 3VSB (Front Panel Power) |
| 3 | NC | Key | 4 | PWR | 5VSB (ID LED Anode) |
| 5 | I | FP_PWR_LED_N | 6 | I | FP_ID_LED_N |
| 7 | PWR | 3.3V (HDD Activity LED Anode) | 8 | I | LED_STATUS_GREEN_N |
| 9 | I | LED_HDD_ACTIVITY_N | 10 | I | LED_STATUS_AMBER_N |
| 11 | O | FP_PWR_BTN_N | 12 | I | LED_NIC1_ACT_N |
| 13 | GND | GND (Power Button GND) | 14 | I | LED_NIC1_LINK_N |
| 15 | O | SYS_RESET | 16 | IO | SMB_SDA |
| 17 | GND | GND (Reset GND) | 18 | I | SMB_SCL |
| 19 | O | FP_ID_BTN_N | 20 | O | FM_INTRUDER_N |
| 21 | IO | Pull-up (1-wire Temp Sensor) | 22 | I | LED_NIC2_ACT_N |
| 23 | O | FP_NMI_BTN_N | 24 | I | LED_NIC2_LINK_N |

## 8.4.1    Power/Sleep Button and LED Support

Pressing the Power button will toggle the system power on and off. This button also functions as a sleep button if enabled by an ACPI compliant operating system. Pressing this button will send a signal to the integrated BMC, which will power on or power off the system. The power LED is a single color and is capable of supporting different indicator states as defined in the following table.

**Table 34. Power/Sleep LED Functional States**

| State | Power Mode | LED | Description |
|-----|-----|-----|-----|
| Power-off | Non-ACPI | Off | System power is off, and the BIOS has not initialized the chipset. |
| Power-on | Non-ACPI | On | System power is on |
| S5 | ACPI | Off | Mechanical is off, and the operating system has not saved any context to the hard disk. |
| S4 | ACPI | Off | Mechanical is off. The operating system has saved context to the hard disk. |
| S3-S1 | ACPI | Slow blink | DC power is still on. The operating system has saved context and gone into a level of low-power state. |
| S0 | ACPI | Steady on | System and the operating system are up and running. |

## 8.4.2    System ID Button and LED Support

Pressing the System ID Button will toggle both the ID LED on the front panel and the Blue ID LED on the server board on and off. The System ID LED is used to identify the system for maintenance when installed in a rack of similar server systems. The System ID LED can also be toggled on and off remotely using the *IPMI Chassis Identify* command which will cause the LED to blink for 15 seconds.

### 8.4.3     System Reset Button Support

When pressed, this button will reboot and re-initialize the system.

### 8.4.4     NMI Button Support

When the NMI button is pressed, it puts the server in a halt state and causes the BMC to issue a non-maskable interrupt (NMI).  This can be useful when performing diagnostics for a given issue where a memory download is necessary to help determine the cause of the problem. Once an NMI has been generated by the BMC, the BMC does not generate another NMI until the system has been reset or powered down.

- The following actions cause the BMC to generate an NMI pulse:
- Receiving a *Chassis Control command* to pulse the diagnostic interrupt. This command does not cause an event to be logged in the SEL.

Watchdog timer pre-timeout expiration with NMI/diagnostic interrupt pre-timeout action enabled.

The following table describes behavior regarding NMI signal generation and event logging by the BMC.

**Table 35. NMI Signal Generation and Event Logging**

| Causal Event | NMI | |
| --- | --- | --- |
| | Signal Generation | Front Panel Diag Interrupt Sensor Event Logging Support |
| Chassis Control command (pulse diagnostic interrupt) | X | – |
| Front panel diagnostic interrupt button pressed | X | X |
| Watchdog Timer pre-timeout expiration with NMI/diagnostic interrupt action | X | X |

### 8.4.5     NIC Activity LED Support

The Front Control Panel includes an activity LED indicator for each on-board Network Interface Controller (NIC).  When a network link is detected, the LED will turn on solid. The LED will blink once network activity occurs at a rate that is consistent with the amount of network activity that is occurring.

### 8.4.6     Hard Drive Activity LED Support

The drive activity LED on the front panel indicates drive activity from the on-board hard disk controllers. The server board also provides a header giving access to this LED for add-in controllers.

### 8.4.7     System Status LED Support

The System Status LED is a bi-color (Green/Amber) indicator that shows the current health of the server system. The system provides two locations for this feature; one is located on the Front Control Panel, the other is located on the back edge of the server board, viewable from the back of the system.  Both LEDs are tied together and will show the same state. The System Status LED states are driven by the on-board platform management sub-system.

## 8.5 I/O Connectors

### 8.5.1 VGA Connector

The following table details the pin-out definition of the VGA connector.

**Table 36. VGA Connector Pin-out (J8A1)**

| Pin | IO | Signal Name |
|-----|------|------------------|
| 1 | A/O | V_IO_R |
| 2 | A/O | V_IO_G |
| 3 | A/O | V_IO_B |
| 4 | NC | TP_VGA_J_4 |
| 5 | GND | GND |
| 6 | GND | GND |
| 7 | GND | GND |
| 8 | GND | GND |
| 9 | NC | TP_VGA_J11_9 |
| 10 | GND | GND |
| 11 | NC | TP_VGA_J_11 |
| 12 | IO | V_BMC_5V_DDC_SDA |
| 13 | I | V_IO_HSYN |
| 14 | I | V_IO_VSYN |
| 15 | I | V_BMC_5V_DDC_SCL |

### 8.5.2 Display Port Connector

The following table details the pin-out definition of the Display Port connector that is only available on S1200SPL.

**Table 37. Display Port Connector Pin-out (J4A1)**

| Pin | IO | Signal Name | Pin | IO | Signal Name |
|-----|------|-------------------|-----|------|------------------|
| 1 | I | DP_DDI_TX_DP0 | 2 | GND | GND |
| 3 | I | DP_DDI_TX_DN0 | 4 | I | DP_DDI_TX_DP1 |
| 5 | GND | GND | 6 | I | DP_DDI_TX_DN1 |
| 7 | I | DP_DDI_TX_DP2 | 8 | GND | GND |
| 9 | I | DP_DDI_TX_DN2 | 10 | I | DP_DDI_TX_DP3 |
| 11 | GND | GND | 12 | I | DP_DDI_TX_DN3 |
| 13 | O | FM_DP_DNG_DETECT | 14 | I | PD_DP_CONFIG2 |
| 15 | IO | DP_AUX_DP | 16 | GND | GND |
| 17 | IO | DP_AUX_DN | 18 | O | FM_DP_HPD_SINK |
| 19 | GND | GND | 20 | PWR | P3V3 |

### 8.5.3 SATA Connectors

The server board S1200SPL provides 8 SATA connectors and, server board S1200SPS provides 6 SATA connectors: SATA-0 (J2K4), SATA-1 (J2K2), SATA-2 (J2K3), SATA-3 (J2K1), SATA-4 (J1K5), SATA-5 (J1K2), SATA-6 (J1K4), and SATA-7 (J1K1).

SATA-4 connector is designed to be compatible with Apacer* SATADOM.

**Table 38. SATA/SATADOM capable Connector Pin-out (J1K4, J1K1, J1K5, J1K2, J2K4, J2K3, J2K1, J2K2)**

| Pin | IO | Signal Name |
|-----|-----|-------------|
| MH1 | PWR | GND |
| 1 | GND | GND |
| 2 | I | SATA_TX_P |
| 3 | I | SATA_TX_N |
| 4 | GND | GND |
| 5 | O | SATA_RX_N |
| 6 | O | SATA_RX_P |
| 7 | PWR | GND |
| MH2 | PWR | P5V (For Apacer* SATADOM)<br>GND (For SATA) |

## 8.5.4　M.2 SATA Connector (J2G1)

The S1200SPL server board supports 22x42mm client M.2 SATA SSD. In order to use M.2 device, a SATA cable need to be connected between any of the SATA connectors (SATA-0 to SATA-7, recommend SATA-7 for better cable routing) and the SATA connector (black) next to the jumpers. See illustration below. The cable shown can be purchased separately.
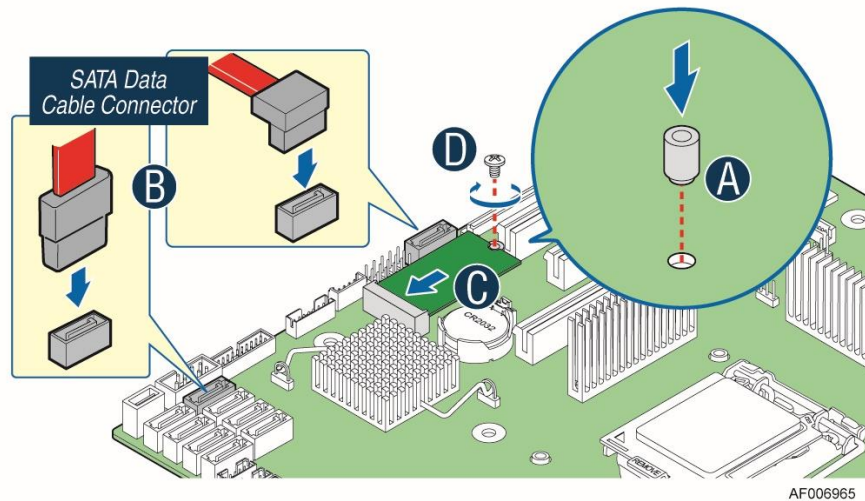


**Figure 19. Installing M.2 Device**

**Table 39. M.2 SATA Connector Pinout**

| Pin | Signal | Signal | Pin |
|---|---|---|---|
| | | GND | 75 |
| 74 | 3.3V | GND | 73 |
| 72 | 3.3V | GND | 71 |
| 70 | 3.3V | PEDET (GND-SATA) | 69 |
| 68 | SUSCLK(32kHz) (I)(0/3.3V) | N/C | 67 |
| | Module Key | Module Key | |
| | Module Key | Module Key | |
| | Module Key | Module Key | |
| | Module Key | Module Key | |
| 58 | Reserved/MFG Clock | GND | 57 |
| 56 | Reserved/MFG Data | N/C | 55 |
| 54 | N/C | N/C | 53 |
| 52 | N/C | GND | 51 |
| 50 | N/C | SATA-A+ | 49 |
| 48 | N/C | SATA-A- | 47 |
| 46 | N/C | GND | 45 |
| 44 | N/C | SATA-B- | 43 |
| 42 | N/C | SATA-B+ | 41 |
| 40 | N/C | GND | 39 |
| 38 | DEVSLP (I)(0/3.3V) | N/C | 37 |
| 36 | N/C | N/C | 35 |
| 34 | N/C | GND | 33 |
| 32 | N/C | N/C | 31 |
| 30 | N/C | N/C | 29 |
| 28 | N/C | GND | 27 |
| 26 | N/C | N/C | 25 |
| 24 | N/C | N/C | 23 |
| 22 | N/C | GND | 21 |
| 20 | N/C | N/C | 19 |
| 18 | 3.3V | N/C | 17 |
| 16 | 3.3V | GND | 15 |
| 14 | 3.3V | N/C | 13 |
| 12 | 3.3V | N/C | 11 |
| 10 | DAS/DSS# (O)(OD) | GND | 9 |
| 8 | N/C | N/C | 7 |
| 6 | N/C | N/C | 5 |
| 4 | 3.3V | GND | 3 |
| 2 | 3.3V | GND | 1 |

## 8.5.5 Serial Port Connector

The server board provides one internal 9-pin Serial header. The following tables define the pin-out.

**Table 40. Internal 9-pin Serial Header Pin-out (J9A1)**

| Pin | IO | Signal Name | Pin | IO | Signal Name |
|---|---|---|---|---|---|

| 1 | O | SPA_DCD | 2 | O | SPA_DSR |
|---|---|---------|---|---|---------|
| 3 | O | SPA_SIN_N | 4 | I | SPA_RTS |
| 5 | I | SPA_SOUT_N | 6 | O | SPA_CTS |
| 7 | I | SPA_DTR | 8 | O | SPA_RI |
| 9 | GND | GND | | | |

## 8.5.6 USB Connector

The Server Board S1200SP Series provide:

- One 2x5 pin USB 2.0 header, providing front panel support for two USB ports respectively
- One 2x10 pin USB 3.0 header on S1200SPL, providing front panel support for two USB 3.0 ports respectively (P4000XXSFDR chassis)
- 2x USB 2.0 ports at the back of the board
- 2x USB 3.0 ports at the back of the board
- 1x internal Type-A USB 2.0 port to support the installation of a USB device inside the server chassis

### Table 41. USB 2.0 FP Header (J1J2)

| Pin | IO | Signal Name | Pin | IO | Signal Name |
|-----|-----|-------------|-----|-----|-------------|
| 1 | PWR | P5V_AUX | 2 | PWR | P5V_AUX |
| 3 | IO | USB_N | 4 | IO | USB_N |
| 5 | IO | USB_P | 6 | IO | USB_P |
| 7 | GND | GND | 8 | GND | GND |
| 9 | NC | Key Pin | 10 | NC | NC |

### Table 42. USB3.0 FP Header (J1J1)

| Pin | IO | Signal Name | Pin | IO | Signal Name |
|-----|-----|-------------|-----|-----|-------------|
| 1 | PWR | P5V_AUX | key | NC | KEY |
| 2 | O | USB3_RX_DN | 19 | PWR | P5V_AUX |
| 3 | O | USB3_RX_DP | 18 | O | USB3_RX_DN |
| 4 | GND | GND | 17 | O | USB3_RX_DP |
| 5 | I | USB3_TX_DN | 16 | GND | GND |
| 6 | I | USB3_TX_DP | 15 | I | USB3_TX_DN |
| 7 | GND | GND | 14 | I | USB3_TX_DP |
| 8 | IO | USB2_DN | 13 | GND | GND |
| 9 | IO | USB2_DP | 12 | IO | USB2_DN |
| 10 | O | TP_USB3_ID | 11 | IO | USB2_DP |

### Table 43. USB 2.0 Connector (Rear IO) (J6A1)

| Pin | IO | Signal Name | Pin | IO | Signal Name |
|-----|-----|-------------|-----|-----|-------------|
| 1 | PWR | P5V_AUX | 5 | PWR | P5V_AUX |
| 2 | IO | USB2_DN | 6 | IO | USB2_DN |
| 3 | IO | USB2_DP | 7 | IO | USB2_DP |
| 4 | GND | GND | 8 | GND | GND |

### Table 44. Internal Type A USB Port Pin-out (J1K3)

| Pin | IO | Signal Name |
|-----|-----|-------------|
| 1 | PWR | P5V_AUX |
| 2 | IO | USB2_DN |
| 3 | IO | USB2_DP |
| 4 | GND | GND |

## 8.5.7    SAS/ROC Module Connector

The S1200SPL server board supports Intel® Integrated RAID Module (known as SAS/ROC module). The SAS/ROC module can be installed to the server board as shown below.
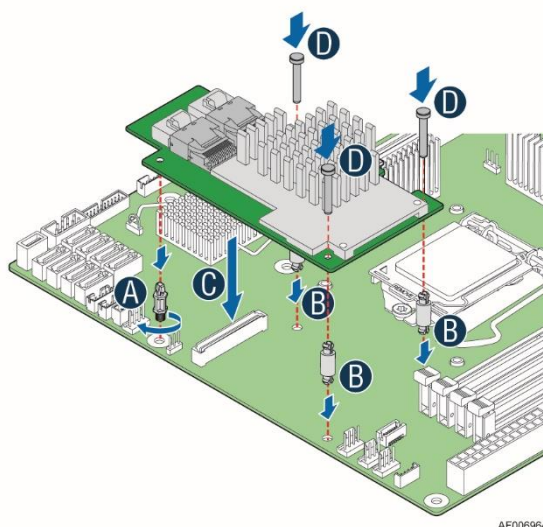


**Figure 20. Installing Intel® Integrated RAID Module**

The following table details the pin-out definition of the SAS/ROC module connector.

**Table 45. I/O Module Connector Pin-out (J4J1)**

| Pin | IO | Signal Name | Pin | IO | Signal Name |
|-----|-----|-------------|-----|-----|-------------|
| 79 | PWR | 3.3V | 80 | PWR | 12V |
| 77 | PWR | 3.3V | 78 | PWR | 12V |
| 75 | PWR | 3.3V | 76 | PWR | 12V |
| 73 | PWR | 3.3V | 74 | PWR | 12V |
| 71 | NC | RSVD_SE | 72 | I | FRU/TEMP ADDR [0] |
| 69 | GND | GND | 70 | PWR | 5V STBY |
| 67 | NC | RSVD_DP | 68 | I | FM_SAS_MODULE_EN_N |
| 65 | NC | RSVD_DN | 66 | PWR | 3.3V STBY |
| 63 | GND | GND | 64 | O | LED_HDD_N |
| 61 | NC | RSVD_DP | 62 | O | FM_SAS_PRESENT_N |
| 59 | NC | RSVD_DN | 60 | O | WAKE# |
| 57 | GND | GND | 58 | I | PERST# |

| Pin | IO | Signal Name | Pin | IO | Signal Name |
|-----|-----|-------------|-----|-----|-------------|
| 55 | I | SMB CLK | 56 | GND | GND |
| 53 | IO | SMB DAT | 54 | I | rSASm REFCLK+ [0] |
| 51 | GND | GND | 52 | I | rSASm REFCLK-  [0] |
| 49 | I | PCIe Gen3 Tn [7] | 50 | GND | GND |
| 47 | I | PCIe Gen3 Tp [7] | 48 | O | PCIe Gen3 Rn [7] |
| 45 | GND | GND | 46 | O | PCIe Gen3 Rp [7] |
| 43 | I | PCIe Gen3 Tn [6] | 44 | GND | GND |
| 41 | I | PCIe Gen3 Tp [6] | 42 | O | PCIe Gen3 Rn [6] |
| 39 | GND | GND | 40 | O | PCIe Gen3 Rp [6] |
| 37 | I | PCIe Gen3 Tn [5] | 38 | GND | GND |
| 35 | I | PCIe Gen3 Tp [5] | 36 | O | PCIe Gen3 Rn [5] |
| 33 | GND | GND | 34 | O | PCIe Gen3 Rp [5] |
| 31 | I | PCIe Gen3 Tn [4] | 32 | GND | GND |
| 29 | I | PCIe Gen3 Tp [4] | 30 | O | PCIe Gen3 Rn [4] |
| 27 | GND | GND | 28 | O | PCIe Gen3 Rp [4] |
| 25 | I | PCIe Gen3 Tn [3] | 26 | GND | GND |
| 23 | I | PCIe Gen3 Tp [3] | 24 | O | PCIe Gen3 Rn [3] |
| 21 | GND | GND | 22 | O | PCIe Gen3 Rp [3] |
| 19 | I | PCIe Gen3 Tn [2] | 20 | GND | GND |
| 17 | I | PCIe Gen3 Tp [2] | 18 | O | PCIe Gen3 Rn [2] |
| 15 | GND | GND | 16 | O | PCIe Gen3 Rp [2] |
| 13 | I | PCIe Gen3 Tn [1] | 14 | GND | GND |
| 11 | I | PCIe Gen3 Tp [1] | 12 | O | PCIe Gen3 Rn [1] |
| 9 | GND | GND | 10 | O | PCIe Gen3 Rp [1] |
| 7 | I | PCIe Gen3 Tn [0] | 8 | GND | GND |
| 5 | I | PCIe Gen3 Tp [0] | 6 | O | PCIe Gen3 Rn [0] |
| 3 | GND | GND | 4 | O | PCIe Gen3 Rp [0] |
| 1 | NC | RSVD_SE | 2 | GND | GND |

## 8.5.8    NIC Connector

**Table 46. NIC Connector Pin-out (JA7A1, J6A2)**

| Pin | IO | Signal Name |
|-----|-----|-------------|
| R1 | PWR | NIC_TRCT |
| R2 | IO | MDI_DP0 |
| R3 | IO | MDI_DN0 |
| R4 | IO | MDI_DP1 |
| R5 | IO | MDI_DN1 |
| R6 | IO | MDI_DP2 |
| R7 | IO | MDI_DN2 |
| R8 | IO | MDI_DP3 |
| R9 | IO | MDI_DN3 |

| Pin | IO | Signal Name |
|-----|-----|-------------|
| R10 | GND | GND |
| L1 | IO | LED2_1G_N |
| L2 | IO | LED2_100M_N |
| L3 | O | LED1_LINK_ACT_N |
| L4 | I | P3V3 |

## 8.6  Fan Headers

The server board provides five SSI-compliant 4-pin fans to use as CPU and I/O cooling fans. 3-pin fans are supported on all fan headers. The pin configuration for each of the 4-pin fan headers is identical and defined in the following tables.

- One 4-pin fan header is designated as processor cooling fan:
  - CPU fan (J7K1)
- Three 4-pin fan headers are designated as system fans:
  - System fan 1 (J3K2)
  - System fan 2 (J8K2)
  - System fan 3 (J8K3)
- One 4-pin fan header is designated as a rear system fan:
  - System fan 4 (J8B1)

The CPU fan and System fans are shown as below.
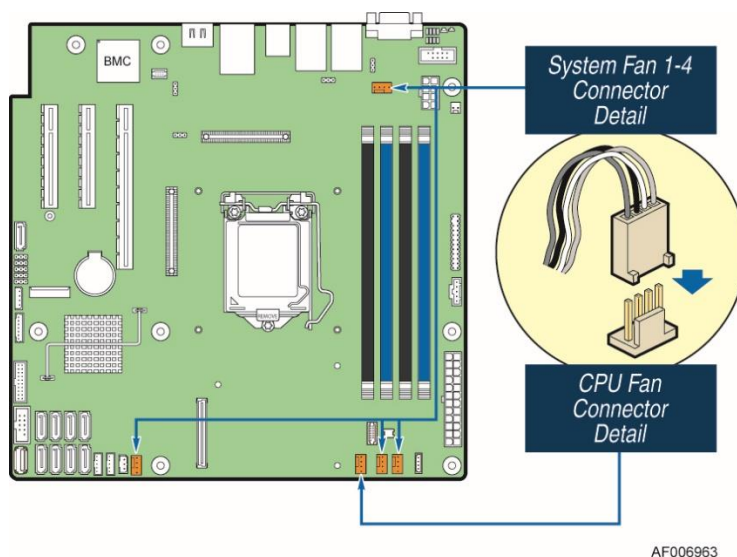


**Figure 21. Fan Headers on the Server Borad**

**Table 47. SSI 4-pin Fan Header Pin-out (J3K2, J8B1, J7K1, J8K2, J8K3)**

| Pin | Signal Name | Type | Description |
|---|---|---|---|
| 1 | Ground | GND | Ground is the power supply ground |
| 2 | 12V | Power | Power supply 12 V |
| 3 | Fan Tach Fan PWM | In Out | FAN_TACH signal is connected to the BMC to monitor the fan speed FAN_PWM signal to control fan speed |
| 4 | Fan PWM Fan Tach | Out In | FAN_PWM signal to control fan speed FAN_TACH signal is connected to the BMC to monitor the fan speed |

*Note: Intel Corporation server boards support peripheral components and can contain a number of high-density VLSI and power delivery components that need adequate airflow to cool. Intel's own chassis are designed and tested to meet the intended thermal requirements of these components when the fully integrated system is used together. It is the responsibility of the system integrator that chooses not to use Intel developed server building blocks to consult vendor datasheets and operating parameters to determine the amount of airflow required for their specific application and environmental conditions. Intel Corporation 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.*

# 9.    Jumper Blocks

The server board includes several 3-pin jumper blocks which are used to as part of a process to restore a board function back to a normal functional state. The following diagram and sections identify the location of each jumper block and provides a description of their use.

The following symbol identifies Pin 1 on each jumper block on the silkscreen:
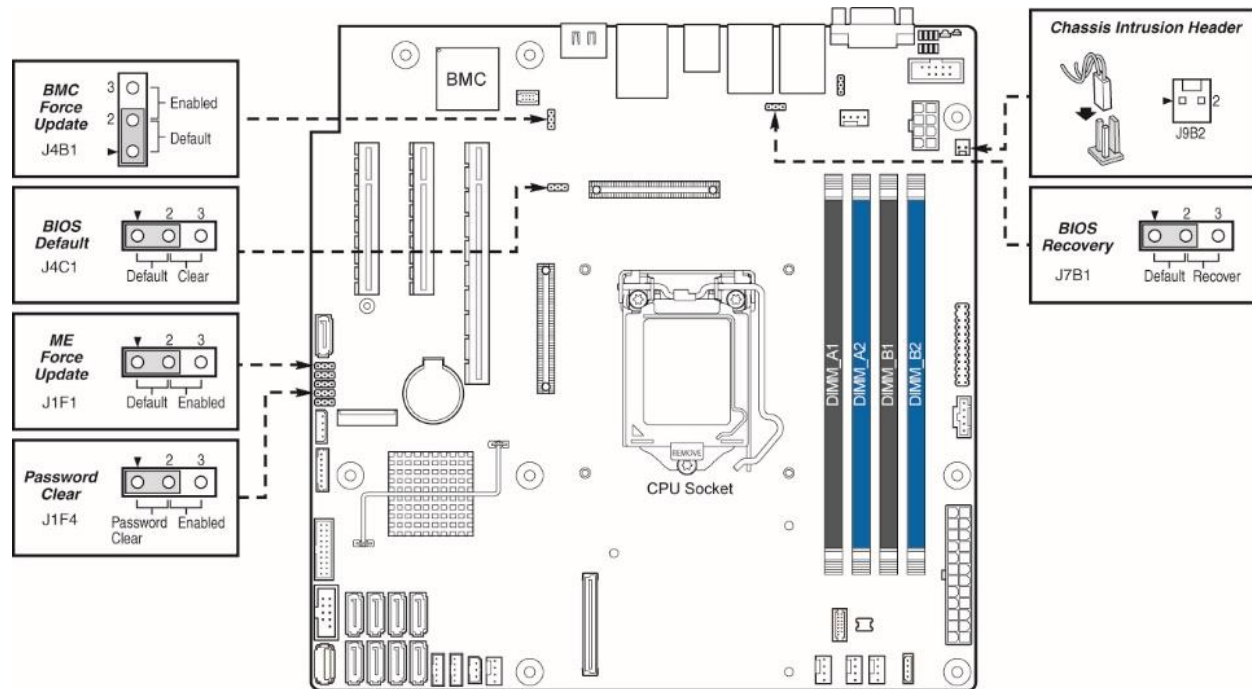


**Figure 22. Jumper Blocks (J4B1, J1F1, J1F4 J7B1, J4C1)**

*Note:*

1. *For safety purposes, the power cord should be disconnected from a system before removing any system components or moving any of the on-board jumper blocks.*

2. *System Update and Recovery files are included in the System Update Packages (SUP) posted to Intel's website.*

**Table 48. Server Board Jumpers (J4B1, J1F1, J1F4, J7B1, J4C1)**

| Jumper Name | Pins | System Results |
|---|---|---|
| J4C1: BIOS Default | 1-2 | These pins should have a jumper in place for normal system operation. (**Default**) |
| | 2-3 | If pins 2-3 are jumpered with AC power plugged in, the CMOS settings clear in 5 seconds. Pins 2-3 should not be jumpered for normal system operation. |
| J7B1: BIOS Recovery | 1-2 | Pins 1-2 should be jumpered for normal system operation. (**Default**) |
| | 2-3 | The main system BIOS does not boot with pins 2-3 jumpered. The system only boots from EFI-bootable recovery media with a recovery BIOS image present. |
| J1F4: Password Clear | 1-2 | These pins should have a jumper in place for normal system operation. |
| | 2-3 | To clear administrator and user passwords, power on the system with pins 2-3 connected. The administrator and user passwords clear in 5-10 seconds after power on. Pins 2-3 should not be connected for normal system operation. |
| J1F1: ME Force Update | 1-2 | ME Firmware Force Update Mode – Disabled (**Default**) |
| | 2-3 | ME Firmware Force Update Mode – Enabled |
| J4B1: BMC Force Update | 1-2 | BMC Firmware Force Update Mode – Disabled (**Default**) |
| | 2-3 | BMC Firmware Force Update Mode – Enabled |

## 9.1    BIOS Default Jumper (J4C1)

1. This jumper resets BIOS Setup options to their default factory settings.

2. Power down the server and unplug the power cords.

3. Open the chassis and remove the Riser #2 assembly.

4. Move BIOS DFLT jumper from the default (pins 1 and 2) position to the Set BIOS Defaults position (pins 2 and 3).

5. Wait 5 seconds then move the jumper back to the default position of pins 1 and 2.

6. Install riser card assembly.

7. Install Power Cords.

8. Power on system.

   *Note: BIOS Error Manager should report a 5220 error code (BIOS Settings reset to default settings).*

## 9.2    BIOS Recovery Jumper (J7B1)

When the BIOS Recovery jumper block is moved from its default pin position, the system will boot into a BIOS Recovery Mode. It is used when the system BIOS has become corrupted and is non-functional, requiring a new BIOS image to be loaded on to the server board.

*Note: The BIOS Recovery jumper is ONLY used to re-install a BIOS image in the event the BIOS has become corrupted.  This jumper is NOT used when the BIOS is operating normally and you need to update the BIOS from one version to another.*

The following steps demonstrate the BIOS recovery process:

1. After downloading the latest System Update Package (SUP) from the Intel® website, copy the following files to the root directory of a USB media device:

- IPMI.EFI

- IFlash32.EFI

- RML.ROM

- ####REC.CAP (where #### = BIOS revision number)

- STARTUP.NSH

2. Power OFF the system.

3. Locate the BIOS Recovery Jumper on the server board and move the jumper block from pins 1–2 (default) to pins 2-3 (recovery setting).

4. Insert the recovery media into a USB port.

5. Power ON the system.

6. The system will automatically boot into the embedded EFI Shell.

7. The STARTUP.NSH file automatically executes and initiates the flash update.  When complete, the IFlash utility will display a message.

8. Power OFF the system and return the BIOS Recovery jumper to its default position.

9. Power ON the system.

10. Do *NOT* interrupt the BIOS POST during the first boot.

11. Configure desired BIOS settings.

## 9.3    Password Clear Jumper (J1F4)

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 creates a security gap until passwords have been installed 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 or by similar means. No method of resetting BIOS configuration settings to default values will affect either the Administrator or User passwords.

1. Power down the server and unplug the power cords.

2. Open the chassis and remove the Riser #2 assembly.

3. Move jumper from the default (pins 1 and 2) operating position to the password clear position (pins 2 and 3).

4. Close the server chassis and reattach the power cords.

5. Power up the server and wait until POST completes.

   *Note: BIOS Error Manager should report a 5224 and 5221 error codes (Password clear jumper is set and Passwords cleared by jumper).*

6. Power down the server and unplug the power cords.

7. Open the chassis, remove the Riser #2 assembly, and move the jumper back to the default position (covering pins 1 and 2).

8. Reinstall the Riser #2 assembly.

9. Close the server chassis and reattach the power cords.

10. Power up the server.

## 9.4    Management Engine (ME) Firmware Force Update Jumper(J1F1)

When the ME Firmware Force Update jumper is moved from its default position, the ME is forced to operate in a reduced minimal operating capacity.  This jumper should only be used if the ME firmware has gotten corrupted and requires re-installation. The following procedure should be followed.

*Note:  System Update and Recovery files are included in the System Update Packages (SUP) posted to Intel's website.*

1.  Turn off the system and remove power cords.
2.  Remove Riser Card Assembly #2.
3.  Move the ME FRC UPD Jumper from the default (pins 1 and 2) operating position to the Force Update position (pins 2 and 3).
4.  Re-attach system power cords.
5.  Power on the system.

    *Note: System Fans will boost and the BIOS Error Manager should report an 83A0 error code (ME in recovery mode).*

6.  Boot to the EFI shell and update the ME firmware using the "MEComplete####.cap" file (where #### = ME revision number) using the following command: iflash32 /u /ni  MEComplete####.cap.
7.  When update has successfully completed, power off system.
8.  Remove AC power cords.
9.  Move ME FRC UPD jumper back to the default position.

    *Note: If the ME FRC UPD jumper is moved with AC power applied, the ME will not operate properly. The system will need have the AC power cords removed, wait for at least 10 seconds and then reinstalled to ensure proper operation.*

10. Install PCI Riser.
11. Install AC power cords.
12. Power on system.

## 9.5    BMC Force Update Jumper (J4B1)

The BMC Force Update jumper is used to put the BMC in Boot Recovery mode for a low-level update.

It is used when the BMC has become corrupted and is non-functional, requiring a new BMC image to be loaded on to the server board.

1.  Turn off the system and remove power cords.
2.  Move the BMC FRC UPDT Jumper from the default (pins 1 and 2) operating position to the Force Update position (pins 2 and 3).
3.  Re-attach system power cords.
4.  Power on the system.

    *Note: System Fans will boost and the BIOS Error Manager should report an 84F3 error code (Baseboard Management Controller in update mode).*

5. Boot to the EFI shell and update the BMC firmware using BMC####.NSH (where #### is the version number of the BMC).

6. When update has successfully completed, power off system.

7. Remove AC power cords.

8. Move BMC FRC UPDT jumper back to the default position.

9. Install AC power cords.

10. Power on system.

11. Boot to the EFI shell and update the FRU and SDR data using FRUSDR####.nsh (where #### is the version number of the FRUSDR package).

12. Reboot the system.

13. Configure desired BMC configuration settings.

# 10. Intel® Light Guided Diagnostics

The server board includes several on-board LED indicators to aid troubleshooting various board level faults. The following figure shows the location for each:
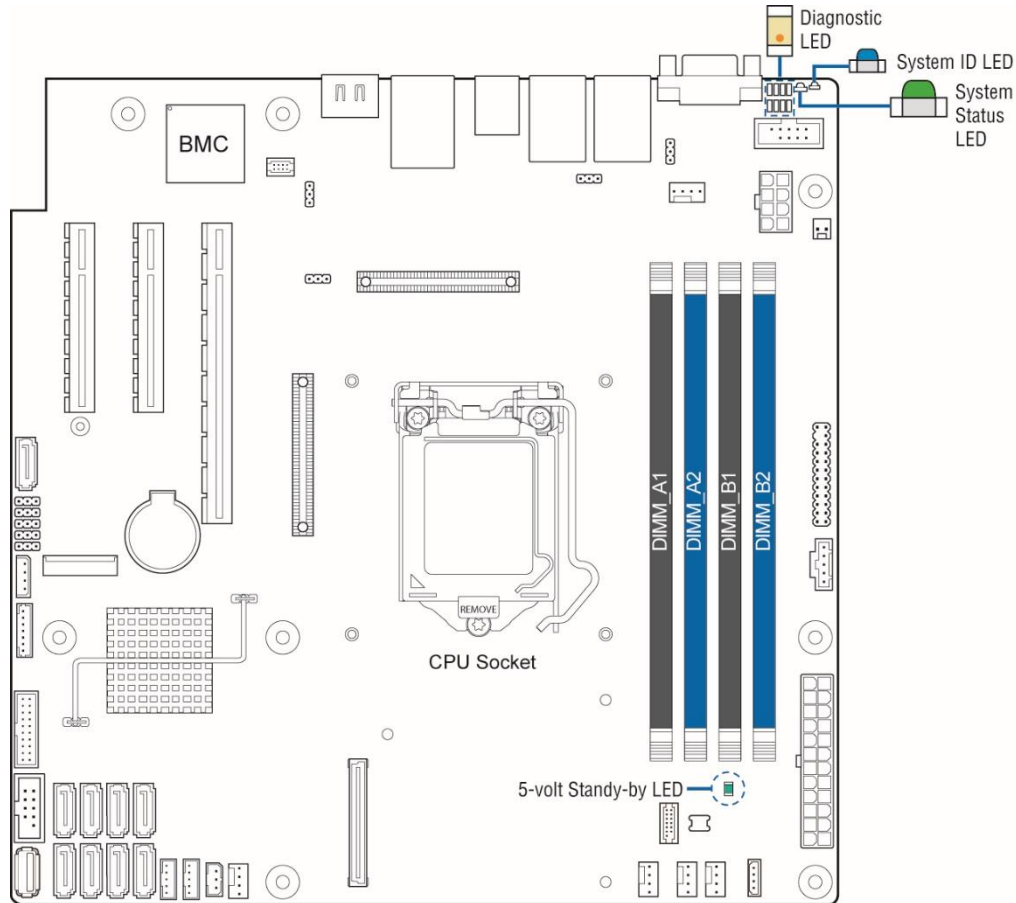


**Figure 23. On-Board LED Placement**

## 10.1 System ID LED

The server board includes a blue system ID LED which is used to visually identify a specific server installed among many other similar servers. There are two options available for illuminating the System ID LED.

1. The front panel ID LED Button is pushed, which causes the LED to illuminate to a solid on state until the button is pushed again.

2. An IPMI Chassis Identify command is remotely entered, which causes the LED to blink.

The System ID LED on the server board is tied directly to the System ID LED on system front panel if present.

## 10.2  System Status LED

The server board includes a bi-color System Status LED. The System Status LED on the server board is tied directly to the System Status LED on the front panel (if present). This LED indicates the current health of the server. Possible LED states include solid green, blinking green, blinking amber, and solid 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 AC 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 will change to solid green.

**Table 49. System Status LED State Definitions**

| Color | State | Criticality | Description |
|---|---|---|---|
| Off | System is not operating | Not ready | 1. System is powered off (AC and/or DC).<br>2. System is in EuP Lot6 Off Mode.<br>3. System is in S5 Soft-Off State.<br>4. System is in S4 Hibernate Sleep State. |
| Green | Solid on | Ok | Indicates that the System is running (in S0 State) and its status is 'Healthy'. The system is not exhibiting any errors. AC power is present and BMC has booted and manageability functionality is up and running. |
| Green | ~1 Hz blink | Degraded - system is operating in a degraded state although still functional, *or* system is operating in a redundant state but with an impending failure warning | System degraded:<br><br>Redundancy loss, such as power-supply or fan. Applies only if the associated platform sub-system has redundancy capabilities.<br><br>Fan warning or failure when the number of fully operational fans is more than minimum number needed to cool the system.<br><br>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.<br><br>Power supply predictive failure occurred while redundant power supply configuration was present.<br><br>Unable to use all of the installed memory (one or more DIMMs failed/disabled but functional memory remains available)<br><br>Correctable Errors over a threshold and migrating to a spare DIMM (memory sparing). This indicates that the user no longer has spared DIMMs indicating a redundancy lost condition. Corresponding DIMM LED lit.<br><br>Uncorrectable memory error has occurred in memory Mirroring Mode, causing Loss of Redundancy.<br><br>Correctable memory error threshold has been reached for a failing DDR4 DIMM when the system is operating in fully redundant RAS Mirroring Mode.<br><br>Battery failure.<br><br>BMC executing in uBoot. (Indicated by Chassis ID blinking at Blinking at 3Hz). System in degraded state (no manageability). BMC uBoot is running but has not transferred control to BMC |

| Color | State | Criticality | Description |
|-------|-------|-------------|-------------|
| | | | Linux*. Server will be in this state 6-8 seconds after BMC reset while it pulls the Linux* image into flash |
| | | | BMC booting Linux*. (Indicated by Chassis ID solid ON). System in degraded state (no manageability). Control has been passed from BMC uBoot to BMC Linux* itself. It will be in this state for ~10-~20 seconds. |
| | | | BMC Watchdog has reset the BMC. |
| | | | Power Unit sensor offset for configuration error is asserted. |
| | | | HDD HSC is off-line or degraded. |
| Amber | ~1 Hz blink | Non-critical - System is operating in a degraded state with an impending failure warning, although still functioning | Non-fatal alarm – 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 |
| | | | Correctable memory error threshold has been reached for a failing DDR4 DIMM when the system is operating in a non-redundant mode |
| Amber | Solid on | Critical, non-recoverable – System is halted | Fatal alarm – system has failed or shutdown: |
| | | | CPU CATERR signal asserted |
| | | | MSID mismatch detected (CATERR also asserts for this case). |
| | | | CPU 1 is missing |
| | | | CPU 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 |
| | | | CPU ERR2 signal asserted |
| | | | BMC\Video memory test failed. (Chassis ID shows blue/solid-on for this condition) |
| | | | Both uBoot BMC FW images are bad. (Chassis ID shows blue/solid-on for this condition) |
| | | | 240VA 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 |

| Color | State | Criticality | Description |
|---|---|---|---|
|  |  |  | Unable to synchronize QPI link frequency |

## 10.3  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.  A BMC boot will occur when AC power is first applied to the system. A BMC reset will occur after: a BMC FW update, upon receiving a BMC cold reset command, and upon a BMC watchdog initiated reset. The following table defines the LED states during the BMC Boot/Reset process.

**Table 50. BMC Boot/Reset Status LED Indicators**

| BMC Boot/Reset State | ID LED | Status LED | Comment |
|---|---|---|---|
| BMC/Video memory test failed | Solid Blue | Solid Amber | Nonrecoverable condition. Contact your Intel® representative for information on replacing this motherboard. |
| Both Universal Bootloader (u-Boot) images bad | Solid Blue | Solid Amber | Nonrecoverable condition. Contact your Intel® representative for information on replacing this motherboard. |
| BMC in u-Boot | Blink Blue 3Hz | Blink Green 1Hz | 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 | Solid green with solid blue 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 per usual. |

## 10.4  Post Code Diagnostic LEDs

A bank of eight POST code diagnostic LEDs are located on the back edge of the server next to the stacked USB connectors. During the system boot process, the BIOS executes a number of platform configuration processes, each of which is assigned a specific hex POST code number. As each configuration routine 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 D for a complete description of how these LEDs are read, and for a list of all supported POST codes.

## 10.5  5 Volt Stand-By Present LED

This LED is illuminated when a power cord (AC or DC) is connected to the server and the power supply is supplying 5 Volt Stand-by power to the server board.  This LED is intended as a service caution indicator to anyone accessing the inside of the server system.

# 11.  Environmental Limits Specification

The following table defines the Intel® Server Board S1200SP series operating and non-operating environmental limits. Operation of the Intel® Server Board S1200SP at conditions beyond those shown in the following table may cause permanent damage to the system. Exposure to absolute maximum rating conditions for extended periods may affect system reliability.

**Table 51. Server Board Design Specifications**

| Operating Temperature | 0º C to 55º C 1 (32º F to 131º F) |
|---|---|
| Non-Operating Temperature | -40º C to 70º C (-40º F to 158º F) |
| DC Voltage | ± 5% of all nominal voltages |
| Shock (Unpackaged) | Trapezoidal, 35g, 170 inches/sec |
| Shock (Packaged)<br>< 20 pounds<br>20 to < 40 pounds<br>40 to < 80 pounds<br>80 to < 100 pounds<br>100 to < 120 pounds<br>120 pounds | 36 inches<br>30 inches<br>24 inches<br>18 inches<br>12 inches<br>9 inches |
| Vibration (Unpackaged) | 5 Hz to 500 Hz 3.13 g RMS random |

*Note:*

*Intel Corporation server boards contain a number of 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 will meet 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 their specific application and environmental conditions. Intel Corporation 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.*

*Disclaimer Note: Intel ensures the unpackaged server board and system meet the shock requirement mentioned above through its own chassis development and system configuration. It is the responsibility of the system integrator to determine the proper shock level of the board and system if the system integrator chooses different system configuration or different chassis. Intel Corporation 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.*

## 11.1  Processor Thermal Design Power (TDP) Support

To allow optimal operation and long-term reliability of Intel® processor-based systems, the processor must remain within the defined minimum and maximum case temperature (TCASE) specifications. Thermal solutions not designed to provide sufficient thermal capability may affect the long-term

reliability of the processor and system. The server board is designed to support the Intel® Xeon® Processor E3-1200 V5 product family TDP guidelines up to and including 80W.

*Disclaimer Note: Intel Corporation server boards contain a number of 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 will meet 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 their specific application and environmental conditions. Intel Corporation cannot be held responsible, if components fail or the server board does not operate correctly when used outside any of their published operating or non-operating limits.*

## 11.2  MTBF

The following is the calculated Mean Time Between Failures (MTBF) 40 degree C (ambient air). These values are derived using a historical failure rate and multiplied by factors for application, electrical and/or thermal stress and for device maturity. You should view MTBF estimates as "reference numbers" only.

- Calculate standard: Telcordia* issue 2
- Calculate Method: Method I-D
- Temperature = 40 degree C
- Environment = GB, GC – Ground Benign, Controlled
- Model = Serial
- Duty cycle = 100%
- Component Quality: Level II
- Adhere to De-rating data

**Table 52. MTBF Estimate**

| Assembly Name | Temperature (Degree C) | MTBF (hours) |
|---|---|---|
| Intel® Server Board S1200SPL | 40 | 1,216,947 |
| Intel® Server Board S1200SPS | 40 | 1,216,947 |

# 12. Server Board Power Distribution

This section provides power supply design guidelines for a system using the Intel® Server Board S1200SP. The following diagram shows the power distribution implemented on this server board.

The power supply data provided in this section is for reference purposes only. It reflects Intel's own DC power out requirements for a CRPS 460W power supply as used in an Intel designed 4U server chassis P4000XXSFDR. The intent of this section is to provide customers with a guide to assist in defining and/or selecting a power supply for custom server platform designs that utilize the server boards detailed in this document.
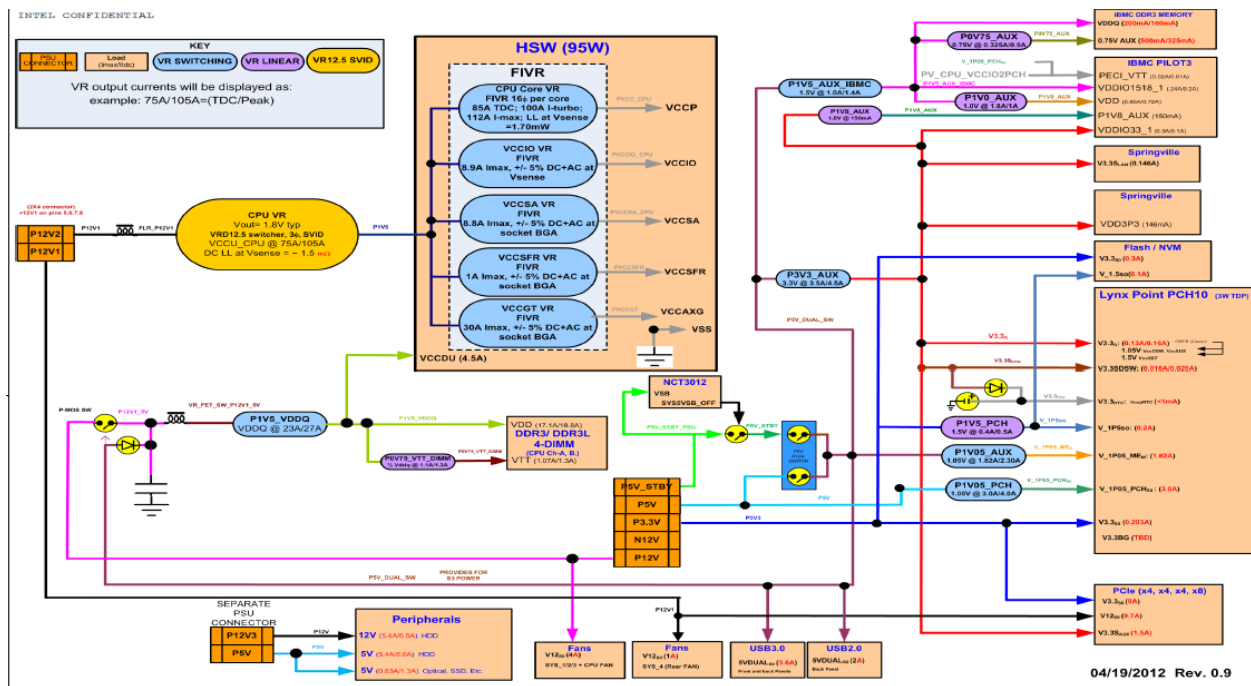


**Figure 24. Power Distribution Block Diagram**

## 12.1 DC Output Specification

### 12.1.1 Output Power/Currents

The following table defines the minimum power and current ratings. The power supply must meet both static and dynamic voltage regulation requirements for all conditions.

**Table 53. Minimum Load Ratings**

| Parameter | Min | Max. | Peak [2, 3] | Unit |
|---|---|---|---|---|
| 12V main | 0.0 | 38.0 | 45.0 | A |
| 12Vstby [1] | 0.0 | 2.1 | 2.4 | A |

*Notes:*

1. *12Vstby must provide 4.0A with two power supplies in parallel. The Fan may start to work when STBY current >1.5A*

2. *Peak combined power for all outputs shall not exceed 575W.*

3. *Length of time peak power can be supported is based on thermal sensor and assertion of the SMBAlert# signal. Minimum peak power duration shall be 20 seconds without asserting the SMBAlert# signal at maximum operating temperature.*

## 12.1.2    Standby Output

The 12VSB output shall be present when an AC input greater than the power supply turn on voltage is applied. There should be load sharing in the standby rail. And two PSU modules should be able to support 4A standby current.

## 12.1.3    Voltage Regulation

The power supply output voltages must stay within the following voltage limits when operating at steady state and dynamic loading conditions.  These limits include the peak-peak ripple/noise.  These shall be measured at the output connectors.

**Table 54. Voltage Regulation Limits**

| PARAMETER | TOLERANCE | MIN | NOM | MAX | UNITS |
|-----------|-----------|-------|--------|--------|-------------|
| +12V      | – 5% / +5% | +11.40 | +12.00 | +12.60 | $V_{rms}$ |
| +12V stby | – 5% / +5% | +11.40 | +12.00 | +12.60 | $V_{rms}$ |

## 12.1.4    Dynamic Loading

The output voltages shall remain within limits specified for the step loading and capacitive loading specified in the table below.  The load transient repetition rate shall be tested between 50Hz and 5kHz at duty cycles ranging from 10%-90%. The load transient repetition rate is only a test specification. The Δ step load may occur anywhere within the MIN load to the MAX load conditions.

**Table 55. Transient Load Requirements**

| Output | Δ Step Load Size | Load Slew Rate | Test capacitive Load |
|--------|------------------|----------------|----------------------|
| +12VSB | 1.0A | 0.25 A/μsec | 20 μF |
| +12V   | 60% of max load | 0.25 A/μsec | 2000 μF |

*Note: For dynamic condition +12V min loading is 1A.*

## 12.1.5    Capacitive Loading

The power supply shall be stable and meet all requirements with the following capacitive loading ranges.

**Table 56. Capacitive Loading Conditions**

| Output | MIN | MAX | Units |
|--------|-----|-----|-------|

| +12VSB | 20 | 3100 | μF |
|---|---|---|---|
| +12V | 500 | 25000 | μF |

## 12.1.6    Grounding

The output ground of the pins of the power supply provides the output power return path.  The output connector ground pins shall be connected to the safety ground (power supply enclosure).  This grounding should be well designed to ensure passing the max allowed Common Mode Noise levels.

The power supply shall be provided with a reliable protective earth ground. All secondary circuits shall be connected to protective earth ground. Resistance of the ground returns to chassis shall not exceed 1.0 mΩ. This path may be used to carry DC current.

## 12.1.7    Closed loop stability

The power supply shall be unconditionally stable under all line/load/transient load conditions including capacitive load ranges specified in Section 12.1.5. A minimum of: **45 degrees phase margin** and -**10dB-gain margin** is required. The power supply manufacturer shall provide proof of the unit's closed-loop stability with local sensing through the submission of Bode plots. Closed-loop stability must be ensured at the maximum and minimum loads as applicable.

## 12.1.8    Residual Voltage Immunity in Standby Mode

The power supply should be immune to any residual voltage placed on its outputs (Typically a leakage voltage through the system from standby output) up to **500mV**. There shall be no additional heat generated, nor stressing of any internal components with this voltage applied to any individual or all outputs simultaneously.  It also should not trip the protection circuits during turn on.

The residual voltage at the power supply outputs for no load condition shall not exceed **100mV** when AC voltage is applied and the PSON# signal is de-asserted.

## 12.1.9    Common Mode Noise

The Common Mode noise on any output shall not exceed **350mV pk-pk** over the frequency band of 10Hz to 20MHz.

1.  The measurement shall be made across a 100Ω resistor between each of DC outputs, including ground at the DC power connector and chassis ground (power subsystem enclosure).
2.  The test set-up shall use a FET probe such as Tektronix model P6046 or equivalent.

## 12.1.10    Soft Starting

The Power Supply shall contain control circuit which provides monotonic soft start for its outputs without overstress of the AC line or any power supply components at any specified AC line or load conditions.

## 12.1.11    Zero Load Stability Requirements

When the power subsystem operates in a no load condition, it does not need to meet the output regulation specification, but it must operate without any tripping of over-voltage or other fault circuitry. When the power subsystem is subsequently loaded, it must begin to regulate and source current without fault.

### 12.1.12    Hot Swap Requirements

Hot swapping a power supply is the process of inserting and extracting a power supply from an operating power system. During this process the output voltages shall remain within the limits with the capacitive load specified. The hot swap test must be conducted when the system is operating under static, dynamic, and zero loading conditions. The power supply shall use a latching mechanism to prevent insertion and extraction of the power supply when the AC power cord is inserted into the power supply.

### 12.1.13    Forced Load Sharing

The +12V output will have active load sharing. The output will share within 10% at full load. The failure of a power supply should not affect the load sharing or output voltages of the other supplies still operating. The supplies must be able to load share in parallel and operate in a hot-swap / redundant **1+1** configurations. The 12VSBoutput is not required to actively share current between power supplies (passive sharing). The 12VSBoutput of the power supplies are connected together in the system so that a failure or hot swap of a redundant power supply does not cause these outputs to go out of regulation in the system.

### 12.1.14    Ripple / Noise

The maximum allowed ripple/noise output of the power supply is defined in the table below. This is measured over a bandwidth of 10Hz to 20MHz at the power supply output connectors. A 10µF tantalum capacitor in parallel with a 0.1µF ceramic capacitor is placed at the point of measurement.

**Table 57. Ripples and Noise**

| +12V main | +12VSB |
|-----------|----------|
| 120mVp-p | 120mVp-p |

The test set-up shall be as shown below.



```
                                     V_OUT
   ○────┌──────────┐                                    ┌──────────┐   LOAD MUST BE
        │ AC HOT   │                                    │   LOAD   │   ISOLATED FROM
        │POWER SUPPLY│                                  │          │   THE GROUND OF
   ○────│AC NEUTRAL│  V_RETURN                          └──────────┘   THE POWER
        └──────────┘              10uF    .1uF                         SUPPLY

              AC GROUND

   GENERAL NOTES:
   1.  LOAD THE OUTPUT WITH ITS MINIMUM
       LOAD CURRENT.
   2.  CONNECT THE PROBES AS SHOWN.
   3.  REPEAT THE MEASUREMENTS WITH THE          ┌──────────┐
       MAXIMUM LOAD ON THE OUTPUT.               │  /\/\/\  │
                                                 │          │
                                                 │  SCOPE   │
                                                 └──────────┘
              SCOPE NOTE:
              USE A TEKTRONIX 7834 OSCILLOSCOPE WITH 7A13 AND
              DIFFERENTIAL PROBE P6055 OR EQUIVALENT.
```

**Figure 25. Differential Noise Test Setup**

*Note: When performing this test, the probe clips and capacitors should be located close to the load.*

These are the timing requirements for the power supply operation. The output voltages must rise from 10% to within regulation limits ($T_{vout\_rise}$) within 5 to 70ms. For 12VSB, it is allowed to rise from 1.0 to 25ms. **All outputs must rise monotonically**. Table below shows the timing requirements for the power supply being turned on and off via the AC input, with PSON held low and the PSON signal, with the AC input applied.

**Table 58. Timing Requirements**

| Item | Description | MIN | MAX | UNITS |
|---|---|---|---|---|
| $T_{vout\_rise}$ | **Output voltage rise time** | 5.0 * | 70 * | ms |
| Tsb_on_delay | **Delay from AC being applied to 12VSBbeing within regulation.** | | 1500 | ms |
| T ac_on_delay | **Delay from AC being applied to all output voltages being within regulation.** | | 3000 | ms |
| Tvout_holdup | **Time 12V output voltage stays within regulation after loss of AC at 70% load.** | 13 | | ms |
| Tpwok_holdup | **Delay from loss of AC to de-assertion of PWOK** | 12 | | ms |
| Tpson_on_delay | **Delay from PSON# active to output voltages within regulation limits.** | 5 | 400 | ms |
| T pson_pwok | **Delay from PSON# deactivate to PWOK being de-asserted.** | | 5 | ms |
| Tpwok_on | **Delay from output voltages within regulation limits to PWOK asserted at turn on.** | 100 | 500 | ms |
| T pwok_off | **Delay from PWOK de-asserted to output voltages dropping out of regulation limits.** | 1 | | ms |
| Tpwok_low | **Duration of PWOK being in the de-asserted state during an off/on cycle using AC or the PSON signal.** | 100 | | ms |
| Tsb_vout | **Delay from 12VSBbeing in regulation to O/Ps being in regulation at AC turn on.** | 50 | 1000 | ms |
| T12VSB_holdup | **Time the 12VSBoutput voltage stays within regulation after loss of AC.** | 70 | | ms |

*Note: The 12VSBoutput voltage rise time shall be from 1.0ms to 25ms*
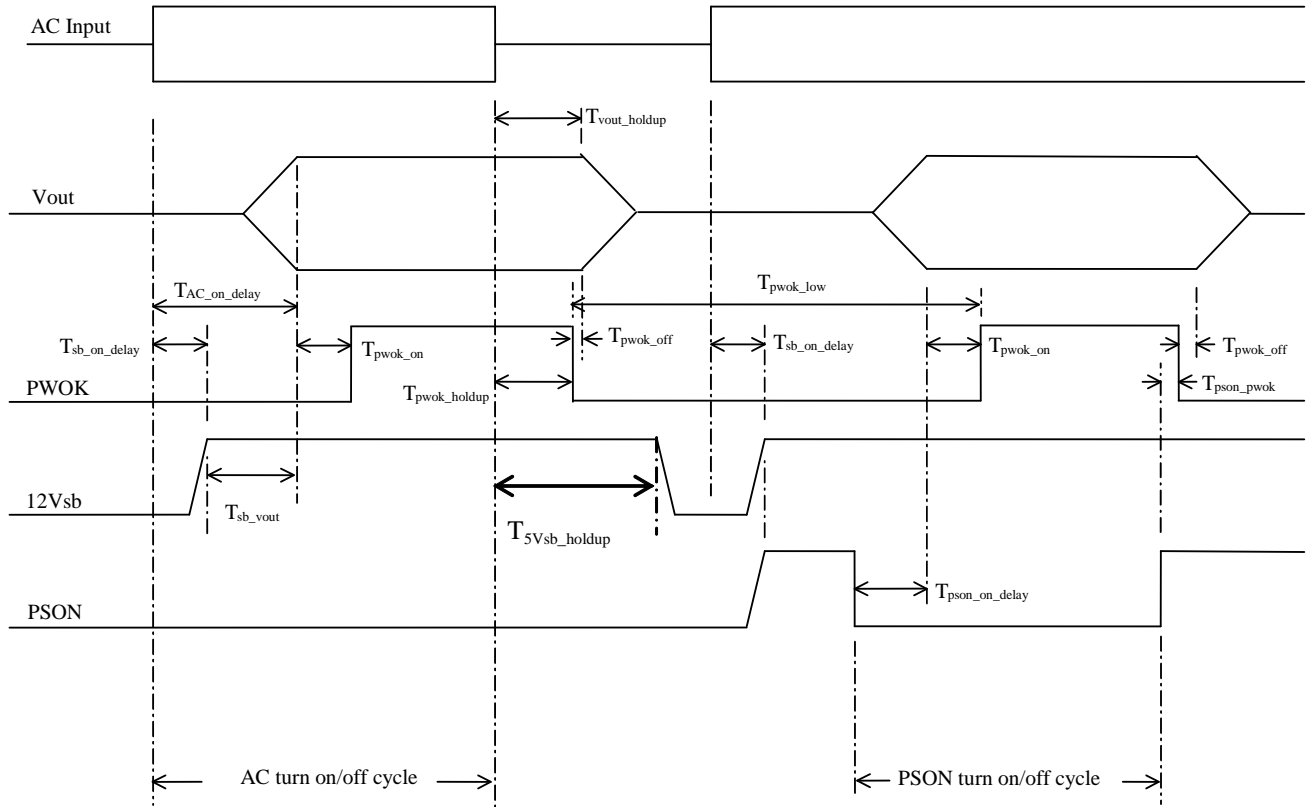
**Figure 26. Turn On/Off Timing (Power Supply Signals)**

## *Appendix A: Integration and Usage Tips*

- When adding or removing components or peripherals from the server board, you must remove AC power cord. With AC power plugged into the server board, 5-V standby is still present even though the server board is powered off.

- This server board supports Intel® Xeon® Processor E3-1200 V5 product family with a Thermal Design Power (TDP) of up to and including 80 Watts. Previous generation Intel® Xeon® processors are not supported.

- On the back edge of the server board are EIGHT diagnostic LEDs that display a sequence of amber POST codes during the boot process. If the server board hangs during POST, the LEDs display the last POST event run before the hang.

- Only Unbuffered DDR4 DIMMs (UDIMMs) are supported on this server board. Mixing of RDIMMs and UDIMMs is not supported.

- Clear CMOS with the AC power cord plugged in. Removing AC power before performing the CMOS Clear operation causes the system to automatically power up and immediately power down after the CMOS Clear procedure is followed and AC power is re-applied. If this happens, remove the AC power cord, wait 30 seconds, and then re-connect the AC power cord. Power up the system and proceed to the **<F2>** BIOS Setup Utility to reset the desired settings.

- Normal BMC functionality is disabled with the Force BMC Update jumper set to the "enabled" position (pins 2-3). You should never run the server with the Force BMC Update jumper set in this position and should only use the jumper in this position when the standard firmware update process fails. This jumper must remain in the default (disabled) position (pins 1-2) when the server is running normally.

- This server board no longer supports the Rolling BIOS (two BIOS banks). It implements the BIOS Recovery mechanism instead.

- When performing a normal BIOS update procedure, you must set the BIOS Recovery jumper to its default position (pins 1-2).

## *Appendix B: Integrated BMC Sensor Tables*

This appendix lists the sensor identification numbers and information about the sensor type, name, supported thresholds, assertion and de-assertion information, and a brief description of the sensor purpose. See the Intelligent Platform Management Interface Specification, Version 2.0 for sensor and event/reading-type table information.

- **Sensor Type**

  The sensor type references the values in the Sensor Type Codes table in the Intelligent Platform Management Interface Specification Second Generation v2.0. It provides a context to interpret the sensor.

- **Event/Reading Type**

  The event/reading type references values from the Event/Reading Type Code Ranges and the Generic Event/Reading Type Code tables in the Intelligent Platform Management Interface Specification Second Generation v2.0. Digital sensors are specific type of discrete sensors that only have two states.

- **Event Thresholds/Triggers**

  The following event thresholds are supported for threshold type sensors:

  - [u,l][nr,c,nc]     upper non-recoverable, upper critical, upper non-critical, lower non-recoverable, lower critical, lower non-critical uc, lc upper critical, lower critical

  Event triggers are supported event-generating offsets for discrete type sensors. The offsets can be found in the *Generic Event/Reading Type Code* or *Sensor Type Code* tables in the *Intelligent Platform Management Interface Specification Second Generation v2.0*, depending on whether the sensor event/reading type is generic or a sensor-specific response.

- **Assertion/De-assertion**

  Assertion and de-assertion indicators reveal the type of events this sensor generates:

  - As: Assertion
  - De: De-assertion

- **Readable Value/Offsets**

  - Readable value indicates the type of value returned for threshold and other non-discrete type sensors.
  - Readable offsets indicate the offsets for discrete sensors that are readable by means of the *Get Sensor Reading* command. Unless otherwise indicated, event triggers are readable. Readable offsets consist of the reading type offsets that do not generate events.

- **Event Data**

  Event data is the data that is included in an event message generated by the associated sensor. For threshold-based sensors, these abbreviations are used:

  - R: Reading value
  - T: Threshold value

- **Rearm Sensors**

The rearm is a request for the event status for a sensor to be rechecked and updated upon a transition between good and bad states. Rearming the sensors can be done manually or automatically. This column indicates the type supported by the sensor. The following abbreviations are used in the comment column to describe a sensor:

- A: Auto-rearm
- M: Manual rearm
- I: Rearm by init agent

▪ **Default Hysteresis**

The hysteresis setting applies to all thresholds of the sensor. This column provides the count of hysteresis for the sensor, which can be 1 or 2 (positive or negative hysteresis).

▪ **Criticality**

Criticality is a classification of the severity and nature of the condition. It also controls the behavior of the front panel status LED.

▪ **Standby**

Some sensors operate on standby power. These sensors may be accessed and/or generate events when the main (system) power is off, but AC power is present.

**Table 59. Integrated BMC Core Sensors**

| Full Sensor Name (Sensor name in SDR) | Sensor # | Platform Applicability | Sensor Type | Event/ Reading Type | Event Offset Triggers | Contrib. To System Status | Assert/ De-assert | Readable Value/ Offsets | Event Data | Rearm | Stand-by |
|---|---|---|---|---|---|---|---|---|---|---|---|
| Power Unit Status (Pwr Unit Status) | 01h | All | Power Unit 09h | Sensor Specific 6Fh | 00 - Power down | OK | As and De | – | Trig Offset | A | X |
| | | | | | 02 - 240 VA power down | Fatal | | | | | |
| | | | | | 04 - A/C lost | OK | | | | | |
| | | | | | 05 - Soft power control failure | Fatal | | | | | |
| | | | | | 06 - Power unit failure | | | | | | |
| Power Unit Redundancy1 (Pwr Unit Redund) | 02h | Chassis-specific | Power Unit 09h | Generic 0Bh | 00 - Fully Redundant | OK | As | – | Trig Offset | M | X |
| | | | | | 01 - Redundancy lost | Degraded | | | | | |
| | | | | | 02 - Redundancy degraded | Degraded | | | | | |
| | | | | | 03 - Non-redundant: sufficient resources. Transition from full redundant state. | Degraded | | | | | |
| | | | | | 04 – Non-redundant: sufficient resources. Transition from insufficient state. | Degraded | | | | | |
| | | | | | 05 - Non-redundant: insufficient resources | Fatal | | | | | |
| | | | | | 06 – Redundant: degraded from fully redundant state. | Degraded | | | | | |
| | | | | | 07 – Redundant: Transition from non-redundant state. | Degraded | | | | | |
| IPMI Watchdog | 03h | All | Watchdog 2 | Sensor Specific | 00 - Timer expired, status only | OK | As | – | | A | X |

| Full Sensor Name (Sensor name in SDR) | Sensor # | Platform Applicability | Sensor Type | Event/ Reading Type | Event Offset Triggers | Contrib. To System Status | Assert/ De-assert | Readable Value/ Offsets | Event Data | Rearm | Stand-by |
|---|---|---|---|---|---|---|---|---|---|---|---|
| (IPMI Watchdog) | | | 23h | 6Fh | 01 - Hard reset | | | | Trig Offset | | |
| | | | | | 02 - Power down | | | | | | |
| | | | | | 03 - Power cycle | | | | | | |
| | | | | | 08 - Timer interrupt | | | | | | |
| Physical Security (Physical Scrty) | 04h | Chassis Intrusion is chassis-specific | Physical Security 05h | Sensor Specific 6Fh | 00 - Chassis intrusion | Degraded OK | As and De | – | Trig Offset | A | X |
| | | | | | 04 - LAN leash lost | | | | | | |
| FP Interrupt (FP NMI Diag Int) | 05h | Chassis - specific | Critical Interrupt 13h | Sensor Specific 6Fh | 00 - Front panel NMI/diagnostic interrupt | OK | As | – | Trig Offset | A | – |
| QPI Correctable Event (QPI Corr Sensor) | 06h | All | Critical Event 13h | 72h | | | | | | | |
| QPI Uncorrectable Event (QPI Fatl Sensor) | 07h | All | Critical Event 13h | 73h | | | | | | | |
| SMI Timeout (SMI Timeout) | 06h | All | SMI Timeout F3h | Digital Discrete 03h | 01 – State asserted | Fatal | As and De | – | Trig Offset | A | – |
| System Event Log (System Event Log) | 07h | All | Event Logging Disabled 10h | Sensor Specific 6Fh | 02 - Log area reset/cleared | OK | As | – | Trig Offset | A | X |

| Full Sensor Name (Sensor name in SDR) | Sensor # | Platform Applicability | Sensor Type | Event/ Reading Type | Event Offset Triggers | Contrib. To System Status | Assert/ De-assert | Readable Value/ Offsets | Event Data | Rearm | Stand-by |
|---|---|---|---|---|---|---|---|---|---|---|---|
| System Event (System Event) | 08h | All | System Event 12h | Sensor Specific 6Fh | 04 – PEF action | OK | As | - | Trig Offset | A | X |
| Button Sensor (Button) | 09h | All | Button/ Switch 14h | Sensor Specific 6Fh | 00 – Power Button 02 – Reset Button | OK | AS | _ | Trig Offset | A | X |
| BMC Watchdog | 0Ah | All | Mgmt System Health 28h | Digital Discrete 03h | 01 – State Asserted | Degraded | As | – | Trig Offset | A | - |
| Voltage Regulator Watchdog (VR Watchdog) | 0Bh | All | Voltage 02h | Digital Discrete 03h | 01 – State Asserted | Fatal | As and De | – | Trig Offset | M | X |
| Fan Redundancy1 (Fan Redundancy) | 0Ch | Chassis-specific | Fan 04h | Generic 0Bh | 00 - Fully redundant | OK | As and De | – | Trig Offset | A | – |
| | | | | | 01 - Redundancy lost | Degraded | | | | | |
| | | | | | 02 - Redundancy degraded | Degraded | | | | | |
| | | | | | 03 - Non-redundant: Sufficient resources. Transition from redundant | Degraded | | | | | |
| | | | | | 04 - Non-redundant: Sufficient resources. Transition from insufficient. | Degraded | | | | | |
| | | | | | 05 - Non-redundant: insufficient resources. | Non-Fatal | | | | | |
| | | | | | 06 – Non-Redundant: degraded from fully redundant. | Degraded | | | | | |

| Full Sensor Name (Sensor name in SDR) | Sensor # | Platform Applicability | Sensor Type | Event/ Reading Type | Event Offset Triggers | Contrib. To System Status | Assert/ De-assert | Readable Value/ Offsets | Event Data | Rearm | Stand-by |
|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | 07 - Redundant degraded from non-redundant | Degraded | | | | | |
| SSB Thermal Trip (SSB Therm Trip) | 0Dh | All | Temperature 01h | Digital Discrete 03h | 01 – State Asserted | Fatal | As and De | – | Trig Offset | M | X |
| IO Module Presence (IO Mod Presence) | 0Eh | Platform-specific | Module /Board 15h | Digital Discrete 08h | 01 – Inserted/Present | OK | As and De | – | Trig Offset | M | - |
| SAS Module Presence (SAS Mod Presence) | 0Fh | Platform-specific | Module /Board 15h | Digital Discrete 08h | 01 – Inserted/Present | OK | As and De | – | Trig Offset | M | X |
| BMC Firmware Health (BMC FW Health) | 10h | All | Mgmt Health 28h | Sensor Specific 6Fh | 04 – Sensor Failure | Degraded | As | - | Trig Offset | A | X |
| System Airflow (System Airflow) | 11h | All | Other Units 0Bh | Threshold 01h | – | – | – | Analog | – | – | – |
| FW Update Status | 12h | All | Version Change 2Bh | OEM defined 70h | 00h – Update started 01h – Update completed successfully. 02h – Update failure | OK | As | _ | Trig Offset | A | – |
| IO Module2 Presence (IO Mod2 Presence) | 13h | Platform-specific | Module /Board 15h | Digital Discrete 08h | 01 – Inserted/Present | OK | As and De | – | Trig Offset | M | - |
| Baseboard Temperature 5 (Platform Specific) | 14h | Platform-specific | Temperature 01h | Threshold 01h | [u,l] [c,nc] | nc = Degraded c = Non-fatal | As and De | Analog | R, T | A | X |

| Full Sensor Name (Sensor name in SDR) | Sensor # | Platform Applicability | Sensor Type | Event/ Reading Type | Event Offset Triggers | Contrib. To System Status | Assert/ De-assert | Readable Value/ Offsets | Event Data | Rearm | Stand-by |
|---|---|---|---|---|---|---|---|---|---|---|---|
| Baseboard Temperature 6 (Platform Specific) | 15h | Platform-specific | Temperature 01h | Threshold 01h | [u,l] [c,nc] | nc = Degraded c = Non-fatal | As and De | Analog | R, T | A | X |
| IO Module2 Temperature (I/O Mod2 Temp) | 16h | Platform-specific | Temperature 01h | Threshold 01h | [u,l] [c,nc] | nc = Degraded c = Non-fatal | As and De | Analog | R, T | A | X |
| PCI Riser 3 Temperature (PCI Riser 3 Temp) | 17h | Platform-specific | Temperature 01h | Threshold 01h | [u,l] [c,nc] | nc = Degraded c = Non-fatal | As and De | Analog | R, T | A | X |
| PCI Riser 4 Temperature (PCI Riser 4 Temp) | 18h | Platform-specific | Temperature 01h | Threshold 01h | [u,l] [c,nc] | nc = Degraded c = Non-fatal | As and De | Analog | R, T | A | X |
| NM Health (NM Health) | 19h | Platform-specific | OEM DCh | OEM defined 73h | - | - | - | - | - | - | – |
| NM Capabilities (NM Capabilities) | 1Ah | Platform-specific | OEM DCh | OEM defined 74h | - | - | - | - | - | - | – |
| Baseboard Temperature 1 (Platform Specific) | 20h | Platform-specific | Temperature 01h | Threshold 01h | [u,l] [c,nc] | nc = Degraded c = Non-fatal | As and De | Analog | R, T | A | X |
| Front Panel Temperature (Front Panel Temp) | 21h | Platform-specific | Temperature 01h | Threshold 01h | [u,l] [c,nc] | nc = Degraded c = Non-fatal | As and De | Analog | R, T | A | X |
| SSB Temperature (SSB Temp) | 22h | All | Temperature | Threshold | [u,l] [c,nc] | nc = Degraded | As and De | Analog | R, T | A | X |

| Full Sensor Name (Sensor name in SDR) | Sensor # | Platform Applicability | Sensor Type | Event/ Reading Type | Event Offset Triggers | Contrib. To System Status | Assert/ De-assert | Readable Value/ Offsets | Event Data | Rearm | Stand-by |
|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | 01h | 01h | | c = Non-fatal | | | | | |
| Baseboard Temperature 2 (Platform Specific) | 23h | Platform-specific | Temperature 01h | Threshold 01h | [u,l] [c,nc] | nc = Degraded c = Non-fatal | As and De | Analog | R, T | A | X |
| Baseboard Temperature 3 (Platform Specific) | 24h | Platform-specific | Temperature 01h | Threshold 01h | [u,l] [c,nc] | nc = Degraded c = Non-fatal | As and De | Analog | R, T | A | X |
| Baseboard Temperature 4 (Platform Specific) | 25h | Platform-specific | Temperature 01h | Threshold 01h | [u,l] [c,nc] | nc = Degraded c = Non-fatal | As and De | Analog | R, T | A | X |
| IO Module Temperature (I/O Mod Temp) | 26h | Platform-specific | Temperature 01h | Threshold 01h | [u,l] [c,nc] | nc = Degraded c = Non-fatal | As and De | Analog | R, T | A | X |
| PCI Riser 1 Temperature (PCI Riser 1 Temp) | 27h | Platform-specific | Temperature 01h | Threshold 01h | [u,l] [c,nc] | nc = Degraded c = Non-fatal | As and De | Analog | R, T | A | X |
| IO Riser Temperature (IO Riser Temp) | 28h | Platform-specific | Temperature 01h | Threshold 01h | [u,l] [c,nc] | nc = Degraded c = Non-fatal | As and De | Analog | R, T | A | X |
| Hot-swap Backplane 1 Temperature (HSBP 1 Temp) | 29h | Chassis-specific | Temperature 01h | Threshold 01h | [u,l] [c,nc] | nc = Degraded c = Non-fatal | As and De | Analog | R, T | A | X |

| Full Sensor Name (Sensor name in SDR) | Sensor # | Platform Applicability | Sensor Type | Event/ Reading Type | Event Offset Triggers | Contrib. To System Status | Assert/ De-assert | Readable Value/ Offsets | Event Data | Rearm | Stand-by |
|---|---|---|---|---|---|---|---|---|---|---|---|
| Hot-swap Backplane 2 Temperature (HSBP 2 Temp) | 2Ah | Chassis-specific | Temperature 01h | Threshold 01h | [u,l] [c,nc] | nc = Degraded c = Non-fatal | As and De | Analog | R, T | A | X |
| Hot-swap Backplane 3 Temperature (HSBP 3 Temp) | 2Bh | Chassis-specific | Temperature 01h | Threshold 01h | [u,l] [c,nc] | nc = Degraded c = Non-fatal | As and De | Analog | R, T | A | X |
| PCI Riser 2 Temperature (PCI Riser 2 Temp) | 2Ch | Platform-specific | Temperature 01h | Threshold 01h | [u,l] [c,nc] | nc = Degraded c = Non-fatal | As and De | Analog | R, T | A | X |
| SAS Module Temperature (SAS Mod Temp) | 2Dh | Platform-specific | Temperature 01h | Threshold 01h | [u,l] [c,nc] | nc = Degraded c = Non-fatal | As and De | Analog | R, T | A | X |
| Exit Air Temperature (Exit Air Temp) | 2Eh | Chassis and Platform Specific | Temperature 01h | Threshold 01h | This sensor does not generate any events. | nc = Degraded c = Non-fatal | As and De | Analog | R, T | A | X |
| Fan Tachometer Sensors2 (Chassis specific sensor names) | 30h–3Fh | Chassis and Platform Specific | Fan 04h | Threshold 01h | [l] [c,nc] | nc = Degraded c = Non-fatal | As and De | Analog | R, T | M | – |
| Fan Present Sensors (Fan x Present) | 40h–4Fh | Chassis and Platform Specific | Fan 04h | Generic 08h | 01 - Device inserted | OK | As and De | - | Triggered Offset | Auto | – |
| Power Supply 1 Status[3] (PS1 Status) | 50h | Chassis-specific | Power Supply 08h | Sensor Specific 6Fh | 00 - Presence | OK | As and De | – | Trig Offset | A | X |
| | | | | | 01 - Failure | Degraded | | | | | |
| | | | | | 02 – Predictive Failure | Degraded | | | | | |

| Full Sensor Name (Sensor name in SDR) | Sensor # | Platform Applicability | Sensor Type | Event/ Reading Type | Event Offset Triggers | Contrib. To System Status | Assert/ De-assert | Readable Value/ Offsets | Event Data | Rearm | Stand-by |
|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | 03 - A/C lost | Degraded | | | | | |
| | | | | | 06 – Configuration error | OK | | | | | |
| Power Supply 2 Status[3] (PS2 Status) | 51h | Chassis-specific | Power Supply 08h | Sensor Specific 6Fh | 00 - Presence | OK | As and De | – | Trig Offset | A | X |
| | | | | | 01 - Failure | Degraded | | | | | |
| | | | | | 02 – Predictive Failure | Degraded | | | | | |
| | | | | | 03 - A/C lost | Degraded | | | | | |
| | | | | | 06 – Configuration error | OK | | | | | |
| Power Supply 1 AC Power Input (PS1 Power In) | 54h | Chassis-specific | Other Units 0Bh | Threshold 01h | [u] [c,nc] | nc = Degraded c = Non-fatal | As and De | Analog | R, T | A | X |
| Power Supply 2 AC Power Input (PS2 Power In) | 55h | Chassis-specific | Other Units 0Bh | Threshold 01h | [u] [c,nc] | nc = Degraded c = Non-fatal | As and De | Analog | R, T | A | X |
| Power Supply 1 +12V % of Maximum Current Output (PS1 Curr Out %) | 58h | Chassis-specific | Current 03h | Threshold 01h | [u] [c,nc] | nc = Degraded c = Non-fatal | As and De | Analog | R, T | A | X |
| Power Supply 2 +12V % of Maximum Current Output (PS2 Curr Out %) | 59h | Chassis-specific | Current 03h | Threshold 01h | [u] [c,nc] | nc = Degraded c = Non-fatal | As and De | Analog | R, T | A | X |
| Power Supply 1 Temperature (PS1 Temperature) | 5Ch | Chassis-specific | Temperature 01h | Threshold 01h | [u] [c,nc] | nc = Degraded c = Non-fatal | As and De | Analog | R, T | A | X |

| Full Sensor Name (Sensor name in SDR) | Sensor # | Platform Applicability | Sensor Type | Event/ Reading Type | Event Offset Triggers | | Contrib. To System Status | Assert/ De-assert | Readable Value/ Offsets | Event Data | Rearm | Stand-by |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Power Supply 2 Temperature (PS2 Temperature) | 5Dh | Chassis-specific | Temperature 01h | Threshold 01h | [u] [c,nc] | | nc = Degraded c = Non-fatal | As and De | Analog | R, T | A | X |
| Hard Disk Drive 15 - 23 Status (HDD 15 - 23 Status) | 60h – 68h | Chassis-specific | Drive Slot 0Dh | Sensor Specific 6Fh | 00 - Drive Presence | | OK | As and De | – | Trig Offset | A | X |
| | | | | | 01- Drive Fault | | Degraded | | | | | X |
| | | | | | 07 - Rebuild/Remap in progress | | Degraded | | | | | |
| Backplane 1 –3 Health Status (HSBP 1 -3 Health) | 69h – 6Bh | Chassis-specific | Micro-controller 16h | Discrete 0Ah | 04-Transition to offline | | Degraded | As and De | - | Trig Offset | A | - |
| Processor 1 Status (P1 Status) | 70h | All | Processor 07h | Sensor Specific 6Fh | 01 - Thermal trip/ FIVR | | Fatal | As and De | – | Trig Offset | M | X |
| | | | | | 07 – Presence | | OK | | | | | |
| Processor 2 Status (P2 Status) | 71h | All | Processor 07h | Sensor Specific 6Fh | 01 - Thermal trip/ FIVR | | Fatal | As and De | – | Trig Offset | M | X |
| | | | | | 07 - Presence | | OK | | | | | |
| Processor 3 Status (P3 Status) | 72h | Platform-specific | Processor 07h | Sensor Specific 6Fh | 01 - Thermal trip | | Fatal | As and De | – | Trig Offset | M | X |
| | | | | | 07 - Presence | | OK | | | | | |
| Processor 4 Status (P4 Status) | 73h | Platform-specific | Processor 07h | Sensor Specific 6Fh | 01 - Thermal trip | | Fatal | As and De | – | Trig Offset | M | X |
| | | | | | 07 - Presence | | OK | | | | | |
| Processor 1 Thermal Margin (P1 Therm Margin) | 74h | All | Temperature 01h | Threshold 01h | - | | - | - | Analog | R, T | A | – |
| Processor 2 Thermal Margin (P2 Therm Margin) | 75h | All | Temperature 01h | Threshold 01h | - | | - | - | Analog | R, T | A | – |

| Full Sensor Name (Sensor name in SDR) | Sensor # | Platform Applicability | Sensor Type | Event/ Reading Type | Event Offset Triggers | Contrib. To System Status | Assert/ De-assert | Readable Value/ Offsets | Event Data | Rearm | Stand-by |
|---|---|---|---|---|---|---|---|---|---|---|---|
| Processor 3 Thermal Margin (P3 Therm Margin) | 76h | Platform-specific | Temperature 01h | Threshold 01h | - | - | - | Analog | R, T | A | – |
| Processor 4 Thermal Margin (P4 Therm Margin) | 77h | Platform-specific | Temperature 01h | Threshold 01h | - | - | - | Analog | R, T | A | – |
| Processor 1 Thermal Control % (P1 Therm Ctrl %) | 78h | All | Temperature 01h | Threshold 01h | [u] [c,nc] | nc = Degraded c = Non-fatal | As and De | Analog | Trig Offset | A | – |
| Processor 2 Thermal Control % (P2 Therm Ctrl %) | 79h | All | Temperature 01h | Threshold 01h | [u] [c,nc] | nc = Degraded c = Non-fatal | As and De | Analog | Trig Offset | A | – |
| Processor 3 Thermal Control % (P3 Therm Ctrl %) | 7Ah | Platform-specific | Temperature 01h | Threshold 01h | [u] [c,nc] | nc = Degraded c = Non-fatal | As and De | Analog | Trig Offset | A | – |
| Processor 4 Thermal Control % (P4 Therm Ctrl %) | 7Bh | Platform-specific | Temperature 01h | Threshold 01h | [u] [c,nc] | nc = Degraded c = Non-fatal | As and De | Analog | Trig Offset | A | – |
| Processor ERR2 Timeout (CPU ERR2) | 7Ch | All | Processor 07h | Digital Discrete 03h | 01 – State Asserted | Fatal | As and De | – | Trig Offset | A | – |
| Catastrophic Error (CATERR) | 80h | All | Processor 07h | Digital Discrete 03h | 01 – State Asserted | Fatal | As and De | – | Trig Offset | M | – |
| MTM Level Change (MTM Lvl Change) | 81h | All | Mgmt Health 28h | Digital Discrete 03h | 01 – State Asserted | - | As and De | – | Trig Offset | A | - |

| Full Sensor Name (Sensor name in SDR) | Sensor # | Platform Applicability | Sensor Type | Event/ Reading Type | Event Offset Triggers | Contrib. To System Status | Assert/ De-assert | Readable Value/ Offsets | Event Data | Rearm | Stand-by |
|---|---|---|---|---|---|---|---|---|---|---|---|
| Processor Population Fault (CPU Missing) | 82h | All | Processor 07h | Digital Discrete 03h | 01 – State Asserted | Fatal | As and De | – | Trig Offset | M | – |
| Processor 1 DTS Thermal Margin (P1 DTS Therm Mgn) | 83h | All | Temperature 01h | Threshold 01h | - | - | - | Analog | R, T | A | – |
| Processor 2 DTS Thermal Margin (P2 DTS Therm Mgn) | 84h | All | Temperature 01h | Threshold 01h | - | - | - | Analog | R, T | A | – |
| Processor 3 DTS Thermal Margin (P3 DTS Therm Mgn) | 85h | Platform Specific | Temperature 01h | Threshold 01h | - | - | - | Analog | R, T | A | – |
| Processor 4 DTS Thermal Margin (P4 DTS Therm Mgn) | 86h | Platform Specific | Temperature 01h | Threshold 01h | - | - | - | Analog | R, T | A | – |
| Auto Config Status (AutoCfg Status) | 87h | All | Mgmt Health 28h | Digital Discrete 03h | 01 – State Asserted | - | As and De | – | Trig Offset | A | - |
| VRD Over Temperature (VRD Hot) | 90h | All | Temperature 01h | Digital Discrete 05h | 01 - Limit exceeded | Non-fatal | As and De | – | Trig Offset | A | – |
| Power Supply 1 Fan Fail 1[3] (PS1 Fan Fail 1) | A0h | Chassis-specific | Fan 04h | Generic – digital discrete 03h | 01 – State Asserted | Non-fatal | As and De | - | Trig Offset | M | X |

| Full Sensor Name (Sensor name in SDR) | Sensor # | Platform Applicability | Sensor Type | Event/ Reading Type | Event Offset Triggers | Contrib. To System Status | Assert/ De-assert | Readable Value/ Offsets | Event Data | Rearm | Stand-by |
|---|---|---|---|---|---|---|---|---|---|---|---|
| Power Supply 1 Fan Fail 2[3] (PS1 Fan Fail 2) | A1h | Chassis-specific | Fan 04h | Generic – digital discrete 03h | 01 – State Asserted | Non-fatal | As and De | - | Trig Offset | M | X |
| PHI 1 Status (GPGPU1 Status) | A2h | Platform Specific | Status C0h | OEM Defined 70h | - | - | - | - | - | - | - |
| PHI 2 Status (GPGPU2 Status) | A3h | Platform Specific | Status C0h | OEM Defined 70h | - | - | - | - | - | - | - |
| Power Supply 2 Fan Fail 1[3] (PS2 Fan Fail 1) | A4h | Chassis-specific | Fan 04h | Generic – digital discrete 03h | 01 – State Asserted | Non-fatal | As and De | - | Trig Offset | M | X |
| Power Supply 2 Fan Fail 2[3] (PS2 Fan Fail 2) | A5h | Chassis-specific | Fan 04h | Generic – digital discrete 03h | 01 – State Asserted | Non-fatal | As and De | - | Trig Offset | M | X |
| PHI 3 Status (GPGPU3 Status) | A6h | Platform Specific | Status C0h | OEM Defined 70h | - | - | - | - | - | - | - |
| PHI 4 Status (GPGPU4 Status) | A7h | Platform Specific | Status C0h | OEM Defined 70h | - | - | - | - | - | - | - |
| PHI 1 Avg Pwr | AAh | Platform Specific | Power 03h | Threshold 01h | - | - | - | Analog | - | - | - |
| PHI 2 Avg Pwr | ABh | Platform Specific | Power 03h | Threshold 01h | - | - | - | Analog | - | - | - |

| Full Sensor Name (Sensor name in SDR) | Sensor # | Platform Applicability | Sensor Type | Event/ Reading Type | Event Offset Triggers | Contrib. To System Status | Assert/ De-assert | Readable Value/ Offsets | Event Data | Rearm | Stand-by |
|---|---|---|---|---|---|---|---|---|---|---|---|
| Processor 1 DIMM Aggregate Thermal Margin 1 (P1 DIMM Thrm Mrgn1) | B0h | All | Temperature 01h | Threshold 01h | [u] [c,nc] | nc = Degraded c = Non-fatal | As and De | Analog | R, T | A | – |
| Processor 1 DIMM Aggregate Thermal Margin 2 (P1 DIMM Thrm Mrgn2) | B1h | All | Temperature 01h | Threshold 01h | [u] [c,nc] | nc = Degraded c = Non-fatal | As and De | Analog | R, T | A | – |
| Processor 2 DIMM Aggregate Thermal Margin 1 (P2 DIMM Thrm Mrgn1) | B2h | All | Temperature 01h | Threshold 01h | [u] [c,nc] | nc = Degraded c = Non-fatal | As and De | Analog | R, T | A | – |
| Processor 2 DIMM Aggregate Thermal Margin 2 (P2 DIMM Thrm Mrgn2) | B3h | All | Temperature 01h | Threshold 01h | [u] [c,nc] | nc = Degraded c = Non-fatal | As and De | Analog | R, T | A | – |
| Processor 3 DIMM Aggregate Thermal Margin 1 (P3 DIMM Thrm Mrgn1) | B4h | Platform Specific | Temperature 01h | Threshold 01h | [u] [c,nc] | nc = Degraded c = Non-fatal | As and De | Analog | R, T | A | – |
| Processor 3 DIMM Aggregate Thermal Margin 2 (P3 DIMM Thrm Mrgn2) | B5h | Platform Specific | Temperature 01h | Threshold 01h | [u] [c,nc] | nc = Degraded c = Non-fatal | As and De | Analog | R, T | A | – |

| Full Sensor Name (Sensor name in SDR) | Sensor # | Platform Applicability | Sensor Type | Event/ Reading Type | Event Offset Triggers | Contrib. To System Status | Assert/ De-assert | Readable Value/ Offsets | Event Data | Rearm | Stand-by |
|---|---|---|---|---|---|---|---|---|---|---|---|
| Processor 4 DIMM Aggregate Thermal Margin 1 (P4 DIMM Thrm Mrgn1) | B6h | Platform Specific | Temperature 01h | Threshold 01h | [u] [c,nc] | nc = Degraded c = Non-fatal | As and De | Analog | R, T | A | – |
| Processor 4 DIMM Aggregate Thermal Margin 2 (P4 DIMM Thrm Mrgn2) | B7h | Platform Specific | Temperature 01h | Threshold 01h | [u] [c,nc] | nc = Degraded c = Non-fatal | As and De | Analog | R, T | A | – |
| Node Auto-Shutdown Sensor (Auto Shutdown) | B8h | Multi-Node Specific | Power Unit 09h | Generic – digital discrete 03h | 01 – State Asserted | Non-fatal | As and De | - | Trig Offset | A | - |
| Fan Tachometer Sensors (Chassis specific sensor names) | BAh–BFh | Chassis and Platform Specific | Fan 04h | Threshold 01h | [l] [c,nc] | nc = Degraded c = Non-fatal2 | As and De | Analog | R, T | M | - |
| Processor 1 DIMM Thermal Trip (P1 Mem Thrm Trip) | C0h | All | Memory 0Ch | Sensor Specific 6Fh | 0A- Critical overtemperature | Fatal | As and De | – | Trig Offset | M | - |
| Processor 2 DIMM Thermal Trip (P2 Mem Thrm Trip) | C1h | All | Memory 0Ch | Sensor Specific 6Fh | 0A- Critical overtemperature | Fatal | As and De | – | Trig Offset | M | - |
| Processor 3 DIMM Thermal Trip (P3 Mem Thrm Trip) | C2h | Platform Specific | Memory 0Ch | Sensor Specific 6Fh | 0A- Critical overtemperature | Fatal | As and De | – | Trig Offset | M | X |

| Full Sensor Name (Sensor name in SDR) | Sensor # | Platform Applicability | Sensor Type | Event/ Reading Type | Event Offset Triggers | Contrib. To System Status | Assert/ De-assert | Readable Value/ Offsets | Event Data | Rearm | Stand-by |
|---|---|---|---|---|---|---|---|---|---|---|---|
| Processor 4 DIMM Thermal Trip (P4 Mem Thrm Trip) | C3h | Platform Specific | Memory 0Ch | Sensor Specific 6Fh | 0A- Critical over temperature | Fatal | As and De | – | Trig Offset | M | X |
| PHI 1 Temp (GPGPU1 Core Temp) | C4h | Platform Specific | Temperature 01h | Threshold 01h | - | - | - | - | - | - | - |
| PHI 2 Temp (GPGPU2 Core Temp) | C5h | Platform Specific | Temperature 01h | Threshold 01h | - | - | - | - | - | - | - |
| PHI 3 Temp (GPGPU3 Core Temp) | C6h | Platform Specific | Temperature 01h | Threshold 01h | - | - | - | - | - | - | - |
| PHI 4 Temp (GPGPU4 Core Temp) | C7h | Platform Specific | Temperature 01h | Threshold 01h | - | - | - | - | - | - | - |
| Global Aggregate Temperature Margin 1 (Agg Therm Mrgn 1) | C8h | Platform Specific | Temperature 01h | Threshold 01h | - | - | - | Analog | R, T | A | – |
| Global Aggregate Temperature Margin 2 (Agg Therm Mrgn 2) | C9h | Platform Specific | Temperature 01h | Threshold 01h | - | - | - | Analog | R, T | A | – |
| Global Aggregate Temperature Margin 3 (Agg Therm Mrgn 3) | CAh | Platform Specific | Temperature 01h | Threshold 01h | - | - | - | Analog | R, T | A | – |
| Global Aggregate Temperature Margin 4 | CBh | Platform Specific | Temperature 01h | Threshold 01h | - | - | - | Analog | R, T | A | – |

| Full Sensor Name (Sensor name in SDR) | Sensor # | Platform Applicability | Sensor Type | Event/ Reading Type | Event Offset Triggers | Contrib. To System Status | Assert/ De-assert | Readable Value/ Offsets | Event Data | Rearm | Stand-by |
|---|---|---|---|---|---|---|---|---|---|---|---|
| (Agg Therm Mrgn 4) | | | | | | | | | | | |
| Global Aggregate Temperature Margin 5 (Agg Therm Mrgn 5) | CCh | Platform Specific | Temperature 01h | Threshold 01h | - | - | - | Analog | R, T | A | – |
| Global Aggregate Temperature Margin 6 (Agg Therm Mrgn 6) | CDh | Platform Specific | Temperature 01h | Threshold 01h | - | - | - | Analog | R, T | A | – |
| Global Aggregate Temperature Margin 7 (Agg Therm Mrgn 7) | CEh | Platform Specific | Temperature 01h | Threshold 01h | - | - | - | Analog | R, T | A | – |
| Global Aggregate Temperature Margin 8 (Agg Therm Mrgn 8) | CFh | Platform Specific | Temperature 01h | Threshold 01h | - | - | - | Analog | R, T | A | – |
| Baseboard +12V (BB +12.0V) | D0h | All | Voltage 02h | Threshold 01h | [u,l] [c,nc] | nc = Degraded c = Non-fatal | As and De | Analog | R, T | A | – |
| Baseboard Temperature 5 (MEM VRM Temp) | D5h | Platform-specific | Temperature 01h | Threshold 01h | [u,l] [c,nc] | nc = Degraded c = Non-fatal | As and De | Analog | R, T | A | X |
| Baseboard Temperature 6 (MEM EFVRD Temp) | D6h | Platform-specific | Temperature 01h | Threshold 01h | [u,l] [c,nc] | nc = Degraded c = Non-fatal | As and De | Analog | R, T | A | X |
| Voltage Fault (Voltage Fault) | D1h | All | Voltage 02h | Discrete 03h | 01 – Asserted | Degraded | - | - | - | A | - |

| Full Sensor Name (Sensor name in SDR) | Sensor # | Platform Applicability | Sensor Type | Event/ Reading Type | Event Offset Triggers | | Contrib. To System Status | Assert/ De-assert | Readable Value/ Offsets | Event Data | Rearm | Stand-by |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Baseboard CMOS Battery (BB +3.3V Vbat) | DEh | All | Voltage 02h | Threshold 01h | [l] [c,nc] | | nc = Degraded c = Non-fatal | As and De | Analog | R, T | A | – |
| Hot-swap Backplane 4 Temperature (HSBP 4 Temp) | E0h | Chassis-specific | Temperature 01h | Threshold 01h | [u,l] [c,nc] | | nc = Degraded c = Non-fatal | As and De | Analog | R, T | A | X |
| Rear Hard Disk Drive 0 -1 Status (Rear HDD 0 - 1 Stat) | E2h - E3h | Chassis-specific | Drive Slot 0Dh | Sensor Specific 6Fh | 00 - Drive Presence | OK | | As and De | – | Trig Offset | A | X |
| | | | | | 01- Drive Fault | Degraded | | | | | | |
| | | | | | 07 - Rebuild/Remap in progress | Degraded | | | | | | |
| Hard Disk Drive 0 - 14 Status (HDD 0 - 14 Status) | F0h - FEh | Chassis-specific | Drive Slot 0Dh | Sensor Specific 6Fh | 00 - Drive Presence | OK | | As and De | – | Trig Offset | A | X |
| | | | | | 01- Drive Fault | Degraded | | | | | | |
| | | | | | 07 - Rebuild/Remap in progress | Degraded | | | | | | |

*Note:*

1. *Redundancy sensors will be only present on systems with appropriate hardware to support redundancy (for instance, fan or power supply). Note that power supply redundancy may be lost even when both supplies are operational if the system is loaded beyond the capacity of a single power supply.*

2. *This is only applicable when the system doesn't support redundant fans. When fan redundancy is supported, then the contribution to system state is driven by the fan redundancy sensor, not individual sensors. On a system with fan redundancy, the individual sensor severities will read the same as the fan redundancy sensor's severity.*

3. *This is only applicable when the system doesn't support redundant power supplies. When redundancy is supported, then the contribution to system state is driven by the power unit redundancy sensor. On a system with power supply redundancy, the individual sensor severities will read the same as the power unit redundancy sensor's severity.*

## *Appendix C: POST Code Diagnostic LED Decoder*

As an aid to assist in trouble shooting a system hang that occurs during a system's Power-On SelfTest (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 a number of memory initialization and platform configuration processes, each of which is assigned a specific hex POST code number. As each routine 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 prior to the error occurring, helping to isolate the possible cause of the hang condition.

Each POST code is represented by eight LEDs; four Green and four Amber. 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 #4, #5, #6, #7. The lower nibble bits are represented by Green Diagnostics LEDs #0, #1, #2 and #3. If the bit is set in the upper and lower nibbles, the corresponding LED is lit. If the bit is clear, the corresponding LED is off.
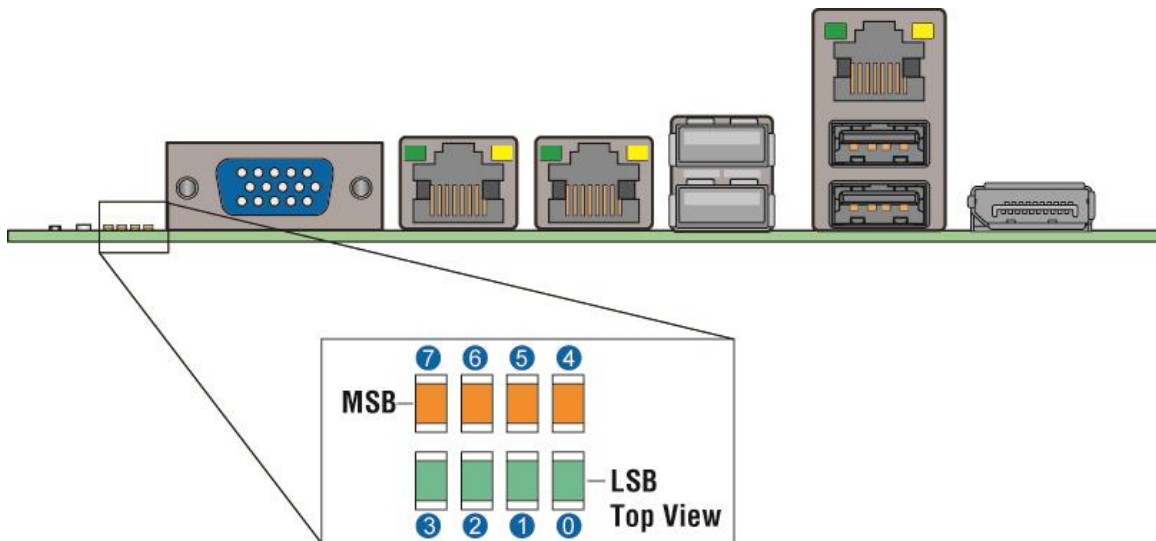


**Figure 27. POST Code Diagnostic LEDs**

In the following example, the BIOS sends a value of ACh to the diagnostic LED decoder. The LEDs are decoded as follows:

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

**Table 60. 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 |
| Results | 1 | 0 | 1 | 0 | 1 | 1 | 0 | 0 |
| | Ah | | | | Ch | | | |

Upper nibble bits = 1010b = Ah; Lower nibble bits = 1100b = Ch; the two are concatenated as ACh

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

**Table 61. POST Progress Codes**

| Checkpoint | Diagnostic LED Decoder 1 = LED On, 0 = LED Off | | | | | | | | Description |
|---|---|---|---|---|---|---|---|---|---|
| | Upper Nibble | | | | Lower Nibble | | | | |
| | MSB | | | | | | | LSB | |
| | 8h | 4h | 2h | 1h | 8h | 4h | 2h | 1h | |
| LED # | #7 | #6 | #5 | #4 | #3 | #2 | #1 | #0 | |
| SEC Phase | | | | | | | | | |
| 01h | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | First POST code after CPU reset |
| 02h | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 0 | Microcode load begin |
| 03h | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 1 | CRAM initialization begin |
| 04h | 0 | 0 | 0 | 0 | 0 | 1 | 0 | 0 | Pei Cache When Disabled |
| 05h | 0 | 0 | 0 | 0 | 0 | 1 | 0 | 1 | SEC Core At Power On Begin. |
| 06h | 0 | 0 | 0 | 0 | 0 | 1 | 1 | 0 | Early CPU initialization during Sec Phase. |
| 07h | 0 | 0 | 0 | 0 | 0 | 1 | 1 | 1 | Early SB initialization during Sec Phase. |
| 08h | 0 | 0 | 0 | 0 | 1 | 0 | 0 | 0 | Early NB initialization during Sec Phase. |
| 09h | 0 | 0 | 0 | 0 | 1 | 0 | 0 | 1 | End Of Sec Phase. |
| 0Eh | 0 | 0 | 0 | 0 | 1 | 1 | 1 | 0 | Microcode Not Found. |
| 0Fh | 0 | 0 | 0 | 0 | 1 | 1 | 1 | 1 | Microcode Not Loaded. |
| PEI Phase | | | | | | | | | |
| 10h | 0 | 0 | 0 | 1 | 0 | 0 | 0 | 0 | PEI Core |
| 11h | 0 | 0 | 0 | 1 | 0 | 0 | 0 | 1 | CPU PEIM |
| 15h | 0 | 0 | 0 | 1 | 0 | 1 | 0 | 1 | NB PEIM |
| 19h | 0 | 0 | 0 | 1 | 1 | 0 | 0 | 1 | SB PEIM |
| MRC Process Codes – MRC Progress Code Sequence is executed | | | | | | | | | |
| PEI Phase continued... | | | | | | | | | |
| 31h | 0 | 0 | 1 | 1 | 0 | 0 | 0 | 1 | Memory Installed |
| 32h | 0 | 0 | 1 | 1 | 0 | 0 | 1 | 0 | CPU PEIM (Cpu Init) |
| 33h | 0 | 0 | 1 | 1 | 0 | 0 | 1 | 1 | CPU PEIM (Cache Init) |
| 4Fh | 0 | 1 | 0 | 0 | 1 | 1 | 1 | 1 | Dxe IPL started |
| DXE Phase | | | | | | | | | |
| 60h | 0 | 1 | 1 | 0 | 0 | 0 | 0 | 0 | DXE Core started |

| Checkpoint | Diagnostic LED Decoder | | | | | | | | Description |
|---|---|---|---|---|---|---|---|---|---|
| | 1 = LED On, 0 = LED Off | | | | | | | | |
| | Upper Nibble | | | | Lower Nibble | | | | |
| | MSB | | | | | | | LSB | |
| | 8h | 4h | 2h | 1h | 8h | 4h | 2h | 1h | |
| LED # | #7 | #6 | #5 | #4 | #3 | #2 | #1 | #0 | |
| 61h | 0 | 1 | 1 | 0 | 0 | 0 | 0 | 1 | DXE NVRAM Init |
| 62h | 0 | 1 | 1 | 0 | 0 | 0 | 1 | 0 | SB RUN Init |
| 63h | 0 | 1 | 1 | 0 | 0 | 0 | 1 | 1 | DXE CPU Init |
| 65h | 0 | 1 | 1 | 0 | 0 | 1 | 0 | 1 | DXE CPU BSP Select |
| 66h | 0 | 1 | 1 | 0 | 0 | 1 | 1 | 0 | DXE CPU AP Init |
| 68h | 0 | 1 | 1 | 0 | 1 | 0 | 0 | 0 | DXE PCI Host Bridge Init |
| 69h | 0 | 1 | 1 | 0 | 1 | 0 | 0 | 1 | DXE NB Init |
| 6Ah | 0 | 1 | 1 | 0 | 1 | 0 | 1 | 0 | DXE NB SMM Init |
| 70h | 0 | 1 | 1 | 1 | 0 | 0 | 0 | 0 | DXE SB Init |
| 71h | 0 | 1 | 1 | 1 | 0 | 0 | 0 | 1 | DXE SB SMM Init |
| 72h | 0 | 1 | 1 | 1 | 0 | 0 | 1 | 0 | DXE SB devices Init |
| 78h | 0 | 1 | 1 | 1 | 1 | 0 | 0 | 0 | DXE ACPI Init |
| 79h | 0 | 1 | 1 | 1 | 1 | 0 | 0 | 1 | DXE CSM Init |
| 80h | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | DXE BDS Started |
| 81h | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | DXE BDS connect drivers |
| 82h | 1 | 0 | 0 | 0 | 0 | 0 | 1 | 0 | DXE PCI Bus begin |
| 83h | 1 | 0 | 0 | 0 | 0 | 0 | 1 | 1 | DXE PCI Bus HPC Init |
| 84h | 1 | 0 | 0 | 0 | 0 | 1 | 0 | 0 | DXE PCI Bus enumeration |
| 85h | 1 | 0 | 0 | 0 | 0 | 1 | 0 | 1 | DXE PCI Bus resource requested |
| 86h | 1 | 0 | 0 | 0 | 0 | 1 | 1 | 0 | DXE PCI Bus assign resource |
| 87h | 1 | 0 | 0 | 0 | 0 | 1 | 1 | 1 | DXE CON_OUT connect |
| 88h | 1 | 0 | 0 | 0 | 1 | 0 | 0 | 0 | DXE CON_IN connect |
| 89h | 1 | 0 | 0 | 0 | 1 | 0 | 0 | 1 | DXE SIO Init |
| 8A | 1 | 0 | 0 | 0 | 1 | 0 | 1 | 0 | DXE USB start |
| 8B | 1 | 0 | 0 | 0 | 1 | 0 | 1 | 1 | DXE USB reset |
| 8C | 1 | 0 | 0 | 0 | 1 | 1 | 0 | 0 | DXE USB detect |
| 8D | 1 | 0 | 0 | 0 | 1 | 1 | 0 | 1 | DXE USB enable |
| 90h | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | DXE IDE begin |
| 91h | 1 | 0 | 0 | 1 | 0 | 0 | 0 | 1 | DXE IDE reset |
| 92h | 1 | 0 | 0 | 1 | 0 | 0 | 1 | 0 | DXE IDE detect |
| 93h | 1 | 0 | 0 | 1 | 0 | 0 | 1 | 1 | DXE IDE enable |
| 94h | 1 | 0 | 0 | 1 | 0 | 1 | 0 | 0 | DXE SCSI begin |
| 95h | 1 | 0 | 0 | 1 | 0 | 1 | 0 | 1 | DXE SCSI reset |
| 96h | 1 | 0 | 0 | 1 | 0 | 1 | 1 | 0 | DXE SCSI detect |
| 97h | 1 | 0 | 0 | 1 | 0 | 1 | 1 | 1 | DXE SCSI enable |
| 98h | 1 | 0 | 0 | 1 | 1 | 0 | 0 | 0 | DXE verifying SETUP password |
| 99h | 1 | 0 | 0 | 1 | 1 | 0 | 0 | 1 | DXE SETUP start |
| 9Ah | 1 | 0 | 0 | 1 | 1 | 0 | 1 | 0 | DXE SETUP input wait |

| Checkpoint | Diagnostic LED Decoder 1 = LED On, 0 = LED Off | | | | | | | | Description |
| | Upper Nibble | | | | Lower Nibble | | | | |
| | MSB | | | | | | | LSB | |
| | 8h | 4h | 2h | 1h | 8h | 4h | 2h | 1h | |
| LED # | #7 | #6 | #5 | #4 | #3 | #2 | #1 | #0 | |
| 9Bh | 1 | 0 | 0 | 1 | 1 | 0 | 1 | 1 | DXE Ready to Boot |
| 9Ch | 1 | 0 | 0 | 1 | 1 | 1 | 0 | 0 | DXE Legacy Boot |
| 9Dh | 1 | 0 | 0 | 1 | 1 | 1 | 0 | 1 | DXE Exit Boot Services |
| C0h | 1 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | RT Set Virtual Address Map Begin |
| C1h | 1 | 1 | 0 | 0 | 0 | 0 | 0 | 1 | RT Set Virtual Address Map End |
| C2h | 1 | 1 | 0 | 0 | 0 | 0 | 1 | 0 | DXE Legacy Option ROM init |
| C3h | 1 | 1 | 0 | 0 | 0 | 0 | 1 | 1 | DXE Reset system |
| C4h | 1 | 1 | 0 | 0 | 0 | 1 | 0 | 0 | DXE USB Hot plug |
| C5h | 1 | 1 | 0 | 0 | 0 | 1 | 0 | 1 | DXE PCI BUS Hot plug |
| C6h | 1 | 1 | 0 | 0 | 0 | 1 | 1 | 0 | DXE NVRAM cleanup |
| C7h | 1 | 1 | 0 | 0 | 0 | 1 | 1 | 1 | DXE Configuration Reset |
| 00h | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | INT19 |
| S3 Resume | | | | | | | | | |
| 40h | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | S3 Resume PEIM (S3 started) |
| 41h | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 1 | S3 Resume PEIM (S3 boot script) |
| 42h | 0 | 1 | 0 | 0 | 0 | 0 | 1 | 0 | S3 Resume PEIM (S3 Video Repost) |
| 43h | 0 | 1 | 0 | 0 | 0 | 0 | 1 | 1 | S3 Resume PEIM (S3 OS wake) |
| BIOS Recovery | | | | | | | | | |
| 46h | 0 | 1 | 0 | 0 | 0 | 1 | 1 | 0 | PEIM which detected forced Recovery condition |
| 47h | 0 | 1 | 0 | 0 | 0 | 1 | 1 | 1 | PEIM which detected User Recovery condition |
| 48h | 0 | 1 | 0 | 0 | 1 | 0 | 0 | 0 | Recovery PEIM (Recovery started) |
| 49h | 0 | 1 | 0 | 0 | 1 | 0 | 0 | 1 | Recovery PEIM (Capsule found) |
| 4Ah | 0 | 1 | 0 | 0 | 1 | 0 | 1 | 0 | Recovery PEIM (Capsule loaded) |

## POST Memory Initialization MRC Diagnostic Codes

There are two types of POST Diagnostic Codes displayed by the MRC during memory initialization; Progress Codes and Fatal Error Codes.

The MRC Progress Codes are displays to the Diagnostic LEDs that show the execution point in the MRC operational path at each step.

**Table 62. MRC Progress Codes**

| Checkpoint | Diagnostic LED Decoder 1 = LED On, 0 = LED Off | | | | | | | | Description |
|---|---|---|---|---|---|---|---|---|---|
| | Upper Nibble | | | | Lower Nibble | | | | |
| | MSB | | | | | | | LSB | |
| | 8h | 4h | 2h | 1h | 8h | 4h | 2h | 1h | |
| LED | #7 | #6 | #5 | #4 | #3 | #2 | #1 | #0 | |
| MRC Progress Codes | | | | | | | | | |
| B0h | 1 | 0 | 1 | 1 | 0 | 0 | 0 | 0 | Detect DIMM population |
| B1h | 1 | 0 | 1 | 1 | 0 | 0 | 0 | 1 | Set DDR4 frequency |
| B2h | 1 | 0 | 1 | 1 | 0 | 0 | 1 | 0 | Gather remaining SPD data |
| B3h | 1 | 0 | 1 | 1 | 0 | 0 | 1 | 1 | Program registers on the memory controller level |
| B4h | 1 | 0 | 1 | 1 | 0 | 1 | 0 | 0 | Evaluate RAS modes and save rank information |
| B5h | 1 | 0 | 1 | 1 | 0 | 1 | 0 | 1 | Program registers on the channel level |
| B6h | 1 | 0 | 1 | 1 | 0 | 1 | 1 | 0 | Perform the JEDEC defined initialization sequence |
| B7h | 1 | 0 | 1 | 1 | 0 | 1 | 1 | 1 | Train DDR4 ranks |
| B8h | 1 | 0 | 1 | 1 | 1 | 0 | 0 | 0 | Initialize CLTT/OLTT |
| B9h | 1 | 0 | 1 | 1 | 1 | 0 | 0 | 1 | Hardware memory test and init |
| BAh | 1 | 0 | 1 | 1 | 1 | 0 | 1 | 0 | Execute software memory init |
| BBh | 1 | 0 | 1 | 1 | 1 | 0 | 1 | 1 | Program memory map and interleaving |
| BCh | 1 | 0 | 1 | 1 | 1 | 1 | 0 | 0 | Program RAS configuration |
| BFh | 1 | 0 | 1 | 1 | 1 | 1 | 1 | 1 | MRC is done |

Memory Initialization at the beginning of POST includes multiple functions, including: 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.

When a major memory initialization error occurs and prevents the system from booting with data integrity, a beep code is generated, the MRC will display 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. The following table lists all MRC fatal errors that are displayed to the Diagnostic LEDs.

**Table 63. POST Progress LED Codes**

| Checkpoint | Diagnostic LED Decoder | | | | | | | | Description |
|---|---|---|---|---|---|---|---|---|---|
| | 1 = LED On, 0 = LED Off | | | | | | | | |
| | Upper Nibble | | | | Lower Nibble | | | | |
| | MSB | | | | | | | LSB | |
| | 8h | 4h | 2h | 1h | 8h | 4h | 2h | 1h | |
| LED | #7 | #6 | #5 | #4 | #3 | #2 | #1 | #0 | |
| MRC Fatal Error Codes | | | | | | | | | |
| E8h | 1 | 1 | 1 | 0 | 1 | 0 | 0 | 0 | No usable memory error<br>01h = No memory was detected from the SPD read, or invalid config that causes no operable memory.<br>02h = Memory DIMMs on all channels of all sockets are disabled due to hardware memtest error.<br>3h = No memory installed. All channels are disabled. |
| E9h | 1 | 1 | 1 | 0 | 1 | 0 | 0 | 1 | Memory is locked by Intel® Trusted Execution Technology and is inaccessible |
| EAh | 1 | 1 | 1 | 0 | 1 | 0 | 1 | 0 | DDR4 channel training error<br>01h = Error on read DQ/DQS (Data/Data Strobe) init<br>02h = Error on Receive Enable<br>3h = Error on Write Leveling<br>04h = Error on write DQ/DQS (Data/Data Strobe |
| EBh | 1 | 1 | 1 | 0 | 1 | 0 | 1 | 1 | Memory test failure<br>01h = Software memtest failure.<br>02h = Hardware memtest failed.<br>03h = Hardware Memtest failure in Lockstep Channel mode requiring a channel to be disabled. This is a fatal error which requires a reset and calling MRC with a different RAS mode to retry. |
| EDh | 1 | 1 | 1 | 0 | 1 | 1 | 0 | 1 | DIMM configuration population error<br>01h = Different DIMM types (UDIMM, RDIMM, LRDIMM) are detected installed in the system.<br>02h = Violation of DIMM population rules.<br>03h = The 3rd DIMM slot cannot be populated when QR DIMMs are installed.<br>04h = UDIMMs are not supported in the 3rd DIMM slot.<br>05h = Unsupported DIMM Voltage. |
| EFh | 1 | 1 | 1 | 0 | 1 | 1 | 1 | 1 | Indicates a CLTT table structure error |

## Appendix D: POST Code Errors

Most error conditions encountered during POST are reported using POST Error Codes. These codes represent specific failures, warnings, or are informational. 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.

The following table lists the supported POST Error Codes. Each error code is assigned an error type which determines the action the BIOS will take when the error is encountered. Error types include Minor, Major, and Fatal. The BIOS action for each is defined as follows:

- **Minor**: The error message is displayed on the screen or on the Error Manager screen, and an error 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:** The error message is displayed on the Error Manager screen, and an error is logged to the SEL. The POST Error **Pause** option setting in the BIOS setup determines whether the system pauses to the Error Manager for this type of error so the user can take immediate corrective action or the system continues booting.

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

- **Fatal**: The system halts during post at a blank screen with the text **"Unrecoverable fatal error found. System will not boot until the error is resolved"** and **"Press <F2> to enter setup"** The POST Error Pause option setting in the BIOS setup does not have any effect with this class of error.

   - When the operator presses the **F2** key on the keyboard, the error message is displayed on the Error Manager screen, and an error is logged to the SEL with the error code. The system cannot boot unless the error is resolved. The user needs to replace the faulty part and restart the system.

*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 will determine which of the listed error codes are supported.*

**Table 64. POST Error Codes and Messages**

| Error Code | Error Message | Response |
|---|---|---|
| 0012 | System RTC date/time not set | Major |
| 0048 | Password check failed | Major |
| 0140 | PCI component encountered a PERR error | Major |
| 0141 | PCI resource conflict | Major |
| 0146 | PCI out of resources error | Major |

| Error Code | Error Message | Response |
| --- | --- | --- |
| 0191 | Processor core/thread count mismatch detected | Fatal |
| 0192 | Processor cache size mismatch detected | Fatal |
| 0194 | Processor family mismatch detected | Fatal |
| 0195 | Processor Intel(R) QPI link frequencies unable to synchronize | Fatal |
| 0196 | Processor model mismatch detected | Fatal |
| 0197 | Processor frequencies unable to synchronize | Fatal |
| 5220 | BIOS Settings reset to default settings | Major |
| 5221 | Passwords cleared by jumper | Major |
| 5224 | Password clear jumper is Set | Major |
| 8130 | Processor 01 disabled | Major |
| 8131 | Processor 02 disabled | Major |
| 8160 | Processor 01 unable to apply microcode update | Major |
| 8161 | Processor 02 unable to apply microcode update | Major |
| 8170 | Processor 01 failed Self Test (BIST) | Major |
| 8171 | Processor 02 failed Self Test (BIST) | Major |
| 8180 | Processor 01 microcode update not found | Minor |
| 8181 | Processor 02 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 | Sensor data record empty | Major |
| 84FF | System event log full | Minor |
| 8500 | Memory component could not be configured in the selected RAS mode | Major |
| 8501 | DIMM Population Error | Major |
| 8520 | DIMM_A1 failed test/initialization | Major |
| 8521 | DIMM_A2 failed test/initialization | Major |
| 8523 | DIMM_B1 failed test/initialization | Major |
| 8524 | DIMM_B2 failed test/initialization | Major |
| 8540 | DIMM_A1 disabled | Major |
| 8541 | DIMM_A2 disabled | Major |
| 8543 | DIMM_B1 disabled | Major |
| 8544 | DIMM_B2 disabled | Major |
| 8560 | DIMM_A1 encountered a Serial Presence Detection (SPD) failure | Major |
| 8561 | DIMM_A2 encountered a Serial Presence Detection (SPD) failure | Major |
| 8563 | DIMM_B1 encountered a Serial Presence Detection (SPD) failure | Major |
| 8564 | DIMM_B2 encountered a Serial Presence Detection (SPD) failure | 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 |
| 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 |
| 92A3 | Serial port component was not detected | Major |

| Error Code | Error Message | Response |
|---|---|---|
| 92A9 | Serial port component encountered a resource conflict error | Major |
| A000 | TPM device not detected. | Minor |
| A001 | TPM device missing or not responding. | Minor |
| A002 | TPM device failure. | Minor |
| A003 | TPM device failed self-test. | Minor |
| 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. | Minor |

## 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 65. POST Error Beep Codes**

| Beeps | Error Message | POST Progress Code | Description |
|---|---|---|---|
| 1 | USB device action | NA | Short beep sounded whenever a USB device is discovered in POST, or inserted or removed during runtime |
| 1 long | Intel® TXT security violation | 0xAE, 0xAF | System halted because Intel® Trusted Execution Technology detected a potential violation of system security. |
| 3 | Memory error | See Tables 28 and 29 | System halted because a fatal error related to the memory was detected. |
| 3-long and 1 | CPU mismatch error | 0xE5, 0xE6 | System haled because fatal error related to the CPU family/core/cache mismatch was detectived |
| 2 | BIOS Recovery started | NA | Recovery boot has been initiated |
| 4 | BIOS Recovery failure | NA | BIOS recovery has failed. This typically happens so quickly after recovery us initiated that it sounds like a 2-4 beep code. |

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 66. Integrated BMC Beep Codes**

| Code | Reason for Beep | Associated Sensors |
|------|-----------------|--------------------|
| 1-5-2-1 | No CPUs installed or first CPU socket is empty. | CPU1 socket is empty, or sockets are populated incorrectly<br>CPU1 must be populated before CPU2. |
| 1-5-2-4 | MSID Mismatch | MSID mismatch occurs if a processor is installed into a system board that has incompatible power capabilities. |
| 1-5-4-2 | Power fault | DC power unexpectedly lost (power good dropout) – Power unit sensors report power unit failure offset |
| 1-5-4-4 | Power control fault (power good assertion timeout). | Power good assertion timeout – Power unit sensors report soft power control failure offset |
| 1-5-1-2 | VR Watchdog Timer sensor assertion | VR controller DC power on sequence was not completed in time. |
| 1-5-1-4 | Power Supply Status | The system does not power on or unexpectedly powers off and a Power Supply Unit (PSU) is present that is an incompatible model with one or more other PSUs in the system. |

## Appendix E: Supported Intel® Server Chassis

The Intel® Server Board S1200SP Family requires an active processor heat sink solution when integrated in the Intel® pedestal server chassis listed below. The Intel® Server Board S1200SP supports up to 80W TDP Intel® Xeon® Processor.

**Table 67. Compatible Intel® Server Chassis P4000S Family**

| Intel® Server Chassis SKU | System Fans | Storage Drives | Power Supply(s) |
|---|---|---|---|
| P4304XXSHCN | One fixed 92x38mm rear system fan | Four 3.5" Hotswap Drive Bays | One 365W non-redundant PSU |
| P4304XXSFCN | One fixed 92x38mm rear system fan | Four 3.5" Fixed Drive Trays | One 365W non-redundant PSU |
| P4000XXSFDR | One fixed 92x38mm rear system fan<br><br>One fixed 92x32mm PCI region fan | Four 3.5" Fixed Drive Trays | Two 460W CRPS PSUs |

You must install the active processor heat sink with the airflow direction as shown in the following figure.
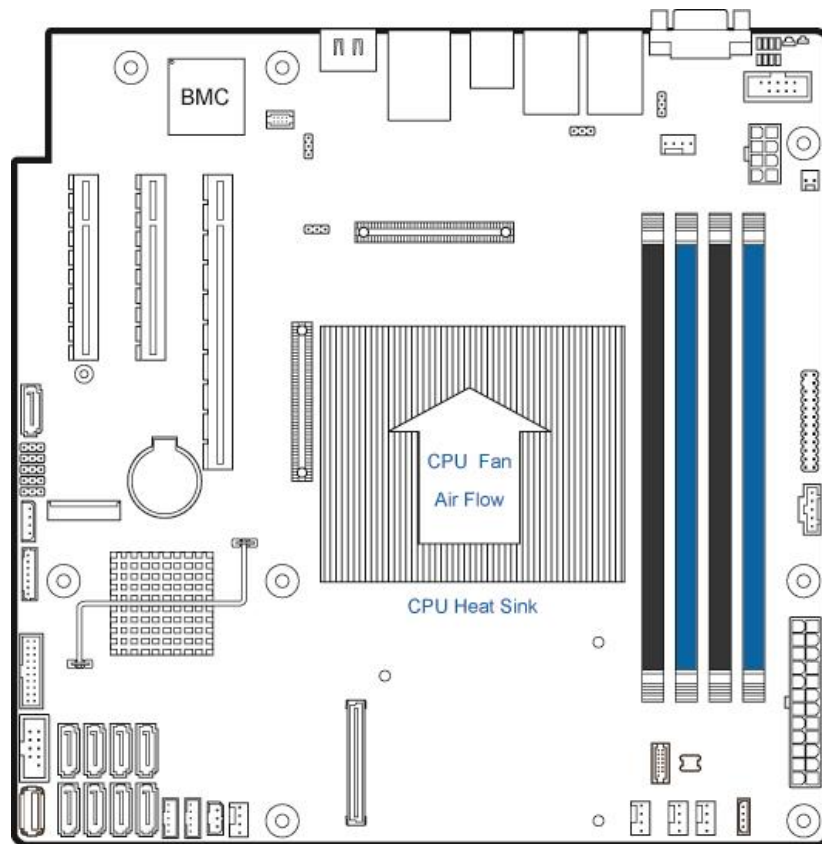


**Figure 28. Processor Heatsink Installation**

# *Glossary*

This appendix contains important terms used in the preceding chapters. For ease of use, numeric entries are listed first (for example, "82460GX") with alpha entries following (for example, "AGP 4x"). Acronyms are then entered in their respective place, with non-acronyms following.

| Term | Definition |
|---|---|
| ACPI | Advanced Configuration and Power Interface |
| AES | Advanced Encryption Standard |
| AMB | Advanced Memory Buffer (there is an AMB on each FBDIMM) |
| APIC | Advanced Programmable Interrupt Controller |
| ARP | Address Resolution Protocol |
| ASF | Alert Standards Forum |
| ASIC | Application specific integrated circuit |
| BIST | Built-in self test |
| BMC | Baseboard management controller |
| Bridge | Circuitry connecting one computer bus to another, allowing an agent on one to access the other. |
| BSP | Bootstrap processor |
| CBC | Chassis bridge controller. A microcontroller connected to one or more other CBCs. Together they bridge the IPMB buses of multiple chassis. |
| CLI | Command-line interface |
| CLTT | Closed-loop thermal throttling (memory throttling mode) |
| CMOS | In terms of this specification, this describes the PC-AT compatible region of battery-backed 128 bytes of memory on the server board. |
| CSR | Control and status register |
| D-cache | Data cache. Processor-local cache dedicated for memory locations explicitly loaded and stored by running code. |
| DHCP | Dynamic Host Configuration Protocol |
| DIB | Device Information Block |
| DPC | Direct Platform Control |
| EEPROM | Electrically erasable programmable read-only memory |
| EMP | Emergency management port |
| EPS | External Product Specification |
| FML | Fast management link |
| FNI | Fast management link network interface |
| FRB | Fault resilient booting |
| FRU | Field replaceable unit |
| FSB | Front side bus |
| FTM | Firmware transfer mode |
| GPIO | General-purpose input/output |
| HSBP | Hot-swap backplane |
| HSC | Hot-swap controller |

| Term | Definition |
|---|---|
| I-cache | Instruction cache. Processor-local cache dedicated for memory locations retrieved through instruction fetch operations. |
| I²C | Inter-integrated circuit bus |
| IA | Intel® architecture |
| IBF | Input buffer |
| ICH | I/O controller hub |
| IERR | Internal error |
| INIT | Initialization signal |
| IPMB | Intelligent Platform Management Bus |
| IPMI | Intelligent Platform Management Interface |
| ITP | In-target probe |
| KCS | Keyboard controller style |
| KT | Keyboard text |
| KVM | Keyboard, video, and mouse |
| LAN | Local area network |
| LCD | Liquid crystal display |
| LPC | Low pin count |
| LUN | Logical unit number |
| MAC | Media Access Control |
| MD5 | Message Digest 5. A hashing algorithm that provides higher security than MD2. |
| MIB | Modular information block. A descriptive text translation of a PET event, contained in a MIB file for use by an SNMP agent hen decoding SEL entries. |
| ms | Millisecond |
| MUX | Multiplexer |
| NIC | Network interface card |
| NMI | Non-maskable interrupt |
| OBF | Output buffer |
| OEM | Original equipment manufacturer |
| OLTT | Open-loop thermal throttling (memory throttling mode) |
| PCI | Peripheral Component Interconnect |
| PECI | Platform Environmental Control Interface |
| PEF | Platform event filtering |
| PET | Platform event trap |
| PIA | Platform information area |
| PLD | Programmable logic device |
| POST | Power-on self-test |
| PROM | Programmable read-only memory |
| PSMI | Power Supply Management Interface |
| PWM | Pulse Width Modulation. The mechanism used to control the speed of system fans. |
| RAM | Random Access Memory |
| RAS | Reliability, availability, and serviceability |

| Term | Definition |
|---|---|
| RC4 | Rivest Cipher 4. A stream cipher designed by Rivest* for RSA data security, now RSA security. It is a variable key-size stream cipher with byte-oriented operations. The algorithm is based on a random permutation. |
| RMCP+ | Remote Management Control Protocol |
| ROM | Read-only memory |
| RTC | Real-time clock |
| SCI | System Control Interrupt. A system interrupt used by hardware to notify the operating system of ACPI events. |
| SDR | Sensor data record |
| SDRAM | Synchronous dynamic random access memory |
| SEL | System event log |
| SHA1 | Secure Hash Algorithm 1 |
| SIO | Server Input/Output |
| SMBus* | A two-wire interface based on the I$^2$C protocol. The SMBus* is a low-speed bus that provides positive addressing for devices and bus arbitration. |
| SMI | Server management interrupt. SMI is the highest priority non-maskable interrupt. |
| SMM | Server management mode |
| SMS | Server management software |
| SNMP | Simple Network Management Protocol |
| SOL | Serial-over-LAN |
| SPT | Straight pass-through |
| SRAM | Static random access memory |
| UART | Universal asynchronous receiver and transmitter |
| UDP | User Datagram Protocol |
| UHCI | Universal Host Controller Interface |
| VLAN | Virtual local area network |

## *Reference Documents*

See the following documents for additional information:

- *Advanced Configuration and Power Interface Specification, Revision 5.0*, http://www.acpi.info/.

- *Intelligent Platform Management Bus Communications Protocol Specification*, Version 1.0. 1998. Intel Corporation, Hewlett-Packard* Company, NEC* Corporation, Dell* Computer Corporation.

- *Intelligent Platform Management Interface Specification, Version 2.0*. 2004. Intel Corporation, Hewlett-Packard* Company, NEC* Corporation, Dell* Computer Corporation.

- *Platform Support for Serial-over-LAN (SOL), TMode, and Terminal Mode External Architecture Specification, Version 1.1*, 02/01/02, Intel Corporation.

- *Intel® Remote Management Module User's Guide*, Intel Corporation.

- *Alert Standard Format (ASF) Specification, Version 2.0*, 23 April 2003, ©2000-2003, Distributed Management Task Force, Inc., http://www.dmtf.org.

- *BIOS for PCSD Platforms Based on Intel® Xeon Processor E3-1200 V5 Product Families External Product Specification*

- *PCSD Platforms Based On Intel Xeon® Processor E3-1200 V5 Product Families BMC Core Firmware External Product Specification*