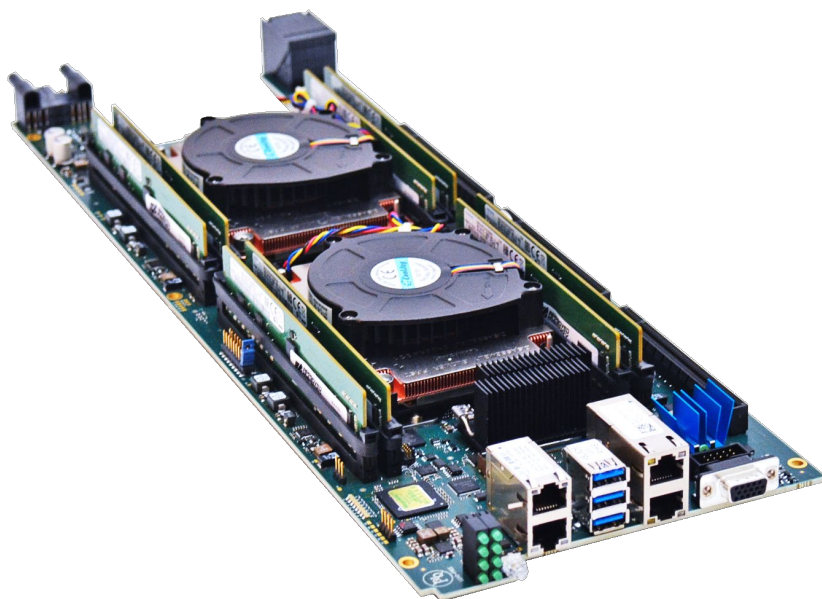




Manual

MSL8256



Prepared by

Trenton Systems
1725 MacLeod Dr
Lawrenceville, GA 30043

Date: August 17, 2020

Model Number: MSL8256

Revision: 2

Table of Contents

Preface.....	2
About Trenton Systems.....	3
Warranty & Policies	4
Handling Precautions.....	7
Regulatory Compliance.....	8
System Overview	11
Diagrams & Layouts	13
Technical Specifications	15



Preface

The information in this user's manual has been carefully reviewed and is believed to be accurate. Trenton Systems assumes no responsibility for any inaccuracies that may be contained in this document and makes no commitment to update or to keep current the information in this manual, or to notify any person or organization of the updates.

Please Note: For the most up-to-date version of this manual, please visit our website at www.trentonsystems.com.

Trenton Systems, Inc. reserves the right to make changes to the product described in this manual at any time and without notice. This product, including software and documentation, is the property of Trenton Systems and/or its licensors, and is supplied only under a license. Any use or reproduction of this product is not allowed, except as expressly permitted by the terms of said license.

IN NO EVENT WILL TRENTON SYSTEMS, INC. BE LIABLE FOR DIRECT, INDIRECT, SPECIAL, INCIDENTAL, SPECULATIVE OR CONSEQUENTIAL DAMAGES ARISING FROM THE USE OR INABILITY TO USE THIS PRODUCT OR DOCUMENTATION, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. IN PARTICULAR, TRENTON SYSTEMS, INC. SHALL NOT HAVE LIABILITY FOR ANY HARDWARE, SOFTWARE, OR DATA STORED OR USED WITH THE PRODUCT, INCLUDING THE COSTS OF REPAIRING, REPLACING, INTEGRATING, INSTALLING OR RECOVERING SUCH HARDWARE, SOFTWARE, OR DATA.

Contact Information

Trenton Systems, Inc.
1725 MacLeod Drive
Lawrenceville, GA 30043
(770) 287-3100

info@trentonsystems.com
sales@trentonsystems.com
support@trentonsystems.com

www.trentonsystems.com



About Trenton Systems

“Unbelievably light. Unquestionably rugged. Undeniably powerful.”

BACKGROUND

Since its establishment in 1989, Trenton Systems has been the leading, high-performance computer hardware and systems manufacturer dedicated to crafting application-specific solutions for the military, industrial and commercial markets. Our rugged computing solutions are designed and manufactured in-house at our state-of-the-art facility in Lawrenceville, Georgia, which we relocated to in 2016 after outgrowing our original facility in Gainesville. Versatile, adaptable and built-to-last, our multi-faceted computing solutions sport completely customizable, ultra-rugged designs, both inside and outside the chassis.

EXPERIENCE

Trenton Systems is trusted by the world’s leading technology companies. Some of our happy customers include Boeing, IBM, L3Harris, Northrop Grumman, Lockheed Martin and Raytheon. We also partner with Intel via the Embedded and Communications Alliance, which provides us with access to Intel’s roadmap, as well as with technical support directly from the company.

Throughout the years, we’ve been at the forefront of the industry in numerous capacities. As a founding member of the PCI Industrial Manufacturers Group (PICMG), we redefined the industry in 1994 with our PICMG 1.0 form factor, and redefined it again in 2005, when we wrote the PICMG 1.3 specification. In 2008, we streamlined our design and manufacturing capabilities, allowing us to craft our systems fully in-house and provide customers with a one-stop shop for all things Trenton rugged.

PHILOSOPHY

Trenton Systems believes in stress-testing and certifying its USA-made products to and beyond the highest military and industrial standards. We believe in crafting solutions that last decades, rather than just a few years. We believe in providing rapid and effective follow-up support so that our customers don’t have to spend hours, days or weeks trying to resolve a simple issue. At Trenton, we believe in setting our customers up for success, both on and off the front lines.



Warranty & Policies

WARRANTY

The following is an abbreviated version of Trenton Systems' warranty policy for processor board products. For a complete warranty statement, contact Trenton Systems or visit our website at www.trentonsystems.com.

Board-level products manufactured by Trenton Systems are warranted against material and manufacturing defects for five years from date of delivery to the original purchaser. Buyer agrees that if this product proves defective Trenton Systems, Inc. is only obligated to repair, replace or refund the purchase price of this product at Trenton Systems' discretion. The warranty is void if the product has been subjected to alteration, neglect, misuse or abuse; if any repairs have been attempted by anyone other than Trenton Systems, Inc.; or if failure is caused by accident, acts of God, or other causes beyond the control of Trenton Systems, Inc. Trenton Systems, Inc. reserves the right to make changes or improvements in any product without incurring any obligation to similarly alter products previously purchased.

In no event shall Trenton Systems, Inc. be liable for any defect in hardware or software or loss or inadequacy of data of any kind, or for any direct, indirect, incidental or consequential damages arising out of or in connection with the performance or use of the product or information provided. Trenton Systems, Inc.'s liability shall in no event exceed the purchase price of the product

RETURN POLICY

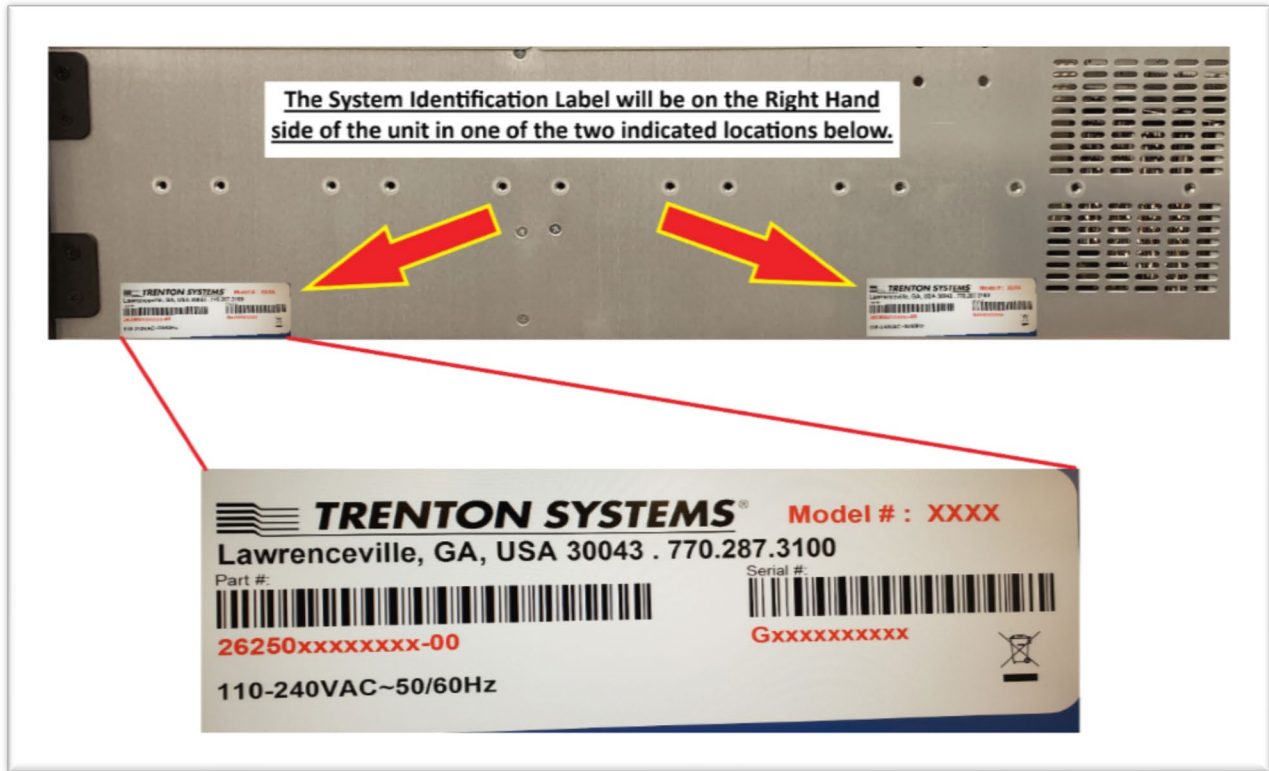
A Service Order Number, obtained from Trenton Systems prior to return, must accompany products returned for repair. The customer must prepay freight on all returned items, and the customer is responsible for any loss or damage caused by common carrier in transit. Items will be returned from Trenton Systems via Ground, unless prior arrangements are made by the customer for an alternative shipping method.

To obtain a Service Order Number, call us at (800) 875-6031 or (770) 287-3100 or email our Technical Support Team at support@trentonsystems.com. We will need the following information:

- ▶ Return company address and contact
- ▶ Model name and model # from the label on the back of the product
- ▶ Part Number and Serial number from the label on the product
- ▶ Description of the failure and failure mode



The Part Number and Serial Number are listed on the chassis as shown here:



Here is an Example label, which shows the Part Number, Revision and Serial Number (S/N):



A Service Order Number will be issued. Mark the Service Order Number clearly on the outside of each box, include a copy of the Service Order failure report for each board and return the product(s) to our Lawrenceville, GA facility:

Trenton Systems, Inc.
1725 MacLeod Drive
Lawrenceville, GA 30043
Attn: Repair Department

TRADEMARKS

- ▶ IBM, PC/AT, VGA, EGA, OS/2 and PS/2 are trademarks or registered trademarks of International Business Machines Corp.



Section 2 / Warranty & Policies

- ▶ AMI and APTIO are trademarks of American Megatrends Inc.
- ▶ Intel, Xeon, Intel Core, Intel AMT, Intel TXT, Intel Hyper-Threading Technology and Intel Virtualization Technology are trademarks or registered trademarks of Intel Corporation.
- ▶ MS-DOS and Microsoft are registered trademarks of Microsoft Corp.
- ▶ PCI Express is a trademark of the PCI-SIG
- ▶ All other brand and product names may be trademarks or registered trademarks of their respective companies.

LIABILITY DISCLAIMER

This manual is as complete and factual as possible at the time of printing; however, the information in this manual may have been updated since that time. Trenton Systems, Inc. reserves the right to change the functions, features or specifications of their products at any time, without notice.

Copyright © 2020 by Trenton Systems, Inc. All rights reserved.

E-mail: support@trentonsystems.com

Web: www.trentonsystems.com



Handling Precautions



WARNING: This product has components that may be damaged by electrostatic discharge.

To protect your processor board from electrostatic damage, be sure to observe the following precautions when handling or storing the system:

- ▶ Keep the processor board in its static-shielded bag until you are ready to perform your installation.
- ▶ Handle the processor board by its edges.
- ▶ Do not touch the I/O connector pins.
- ▶ Do not apply pressure or attach labels to the processor board.
- ▶ Use a grounded wrist strap at your workstation or ground yourself frequently by touching the metal chassis of the system before handling any components. The system must be plugged into an outlet that is connected to an earth ground.
- ▶ Use antistatic padding on all work surfaces.
- ▶ Avoid static-inducing carpeted areas.

Recommended Processor Board Storage Precautions

This SHB has components on both sides of the PCB. Some of these components are extremely small and subject to damage if the board is not handled properly. It is important for you to observe the following precautions when handling or storing the board to prevent components from being damaged or broken off:

- ▶ Store the board in padded shipping material or in an anti-static board rack.
- ▶ Do not place an unprotected board on a flat surface.



WARNING: There is danger of explosion if the CMOS battery is replaced incorrectly. Disposal of battery into fire or a hot oven, or mechanically crushing or cutting of a battery can result in an explosion.



Regulatory Compliance

DECLARATION OF CONFORMITY

FCC

This device complies with part 15 of the FCC rules as a Class A device. Operation is subject to the following two conditions: (1) this device may not cause harmful interference and (2) this device must accept any interference received, including interference that might cause undesired operation.

CE

This equipment complies with all applicable European Union (CE) directives if it has a CE marking. For this device to remain CE compliant, only CE compliant parts can be installed, and proper cables and cabling techniques are required.

AGENCY APPROVALS

All standards should be at applicable revision levels at time of test.

- ▶ Electromagnetic Emissions (EMI)
 - Designed to meet FCC 47 CFR Part 15 Subpart B ISSED Canada ICES-003 Issue 6 Class A as a minimum.
 - Designed to meet Electromagnetic Compatibility Directive 2014/30/EU
 - Immunity Product Standard: EN55035:2017
 - Emissions Product Standards: EN55032:2012, EN 61000-3-2:2014, EN61000-3-3:2013

Safety

- ▶ This product will be UL approvable for safety concerns and designed for IEC 60950-1:2005 and IEC 62368-1:2014

Environmental

- ▶ This product will be approvable for MIL-STD-810G High and Low-Temp Operating and Storage system testing to test methods 501.5 and 502.5, Procedures II and I
- ▶ This product will be approvable for MIL-STD-810G Altitude Operational and Storage system testing to test method 500.5, Procedures II and I.
- ▶ TRC1002 with MSL8256 has been tested to and passed MIL-STD-461G, CE102, and RE102 requirements.



INTRODUCTION

It is important to be aware of the system considerations listed below before installing your MSL8256 (8257-xxx) processor board. Overall system performance may be affected by incorrect usage of these features.

DDR4-2400 MEMORY

Trenton Systems recommends ECC DDR4-2400 PC4-21300 RDIMM memory modules for use on the MSL8256. The MSL8256 supports a maximum of 1TB of memory using eight channels across eight DIMM slots.

NOTES:

- ▶ To maximize memory interface speed, populate each memory channel with DDR4 DIMMs having the same interface speed. The processor board will support DIMMs with different speeds, but the memory channel interface will operate speed of the slowest DIMM.
- ▶ All memory modules must have gold contacts.
- ▶ All memory modules must have a 288-pin edge connector
- ▶ Populate the memory sockets starting with memory channel A and begin by using the DIMM socket closest to the CPU first. Refer to the MSL8256 board layout drawing and populate the memory sockets using the population order illustrated in the chart below:

POPULATION ORDER	CPU0	CPU1
1	BK0	BK4
2	BK2	BK6
3	BK1	BK5
4	BK3	BK7

- ▶ Using a balanced memory population approach ensures maximum memory interface performance. A “balanced approach” means using an even number of DIMMs on the MSL8256 processor board whenever possible.
- ▶ The memory DIMMs on the processor board connect directly to the CPU and at least one memory module must be installed on the board.



SATA RAID OPERATION (WINDOWS O/S SETUP)

The Intel® C622 Platform Controller Hub (PCH) used on the processor board features Intel® Rapid Storage Technology (Intel® RST) and requires unique drivers.

BIOS

The MSL8256 features the Aptio® BIOS from American Megatrends, Inc. (AMI) with a ROM-resident setup utility called the Aptio Text Setup Environment or TSE.

OPERATING SYSTEMS

Trenton Systems has successfully tested the MSL8256 processor board with a wide variety of contemporary operating systems including Linux (Red Hat RHEL, Centos and SUSE), Windows® 8.1, Windows® 10, Windows® 2012 Server, and Windows® 2016 Server.



System Overview

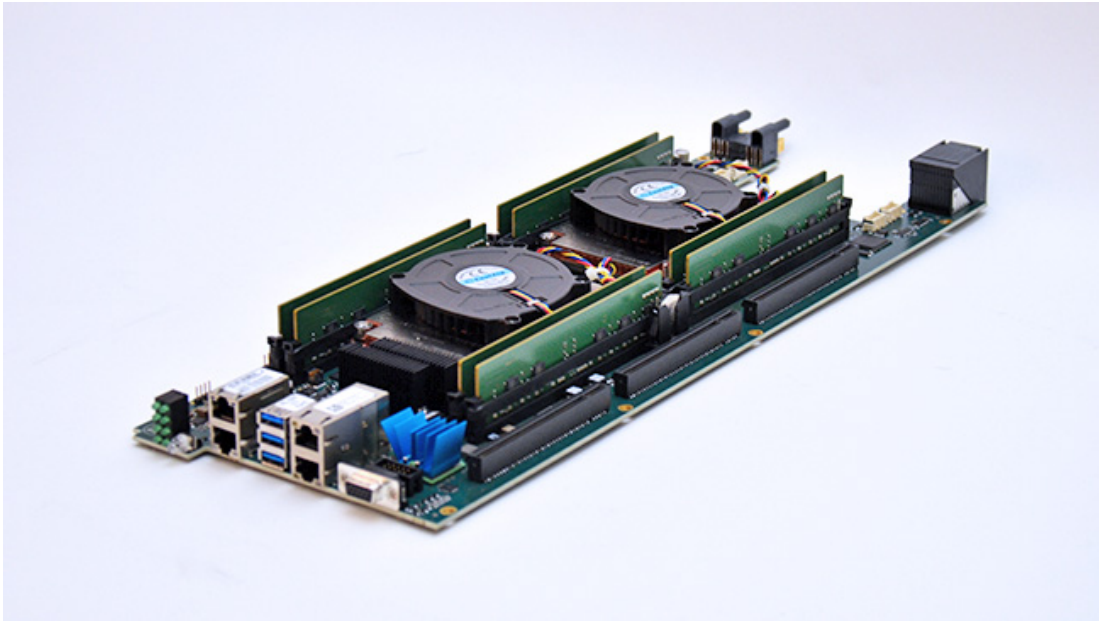


Figure 1: MSL8256

Exceptional performance, modular design and long-life components backed by made in USA reliability.



Section 6 / System Overview

PROCESSOR BOARD

MSL8256

COMPATIBLE CHASSIS MODEL NUMBER(S)

TRC1001, TRC1002, MBS1001, MBS1002, MBS2000, MBS2001

[Contact us for custom options](#)

PROCESSORS

- ▶ Intel® Xeon® Scalable Processors
- ▶ CPU TDP support up to 125W

CPU	ECC	Cores / Threads	Frequency	TDP
Gold 6238T	Yes	22/44	1.90 GHz	125W
Gold 6230	Yes	20/40	2.10 GHz	125W
Gold 6230N	Yes	20/40	2.30 GHz	125W
Gold 5218N	Yes	16/32	2.30 GHz	110W
Silver 4214R	Yes	12/24	2.40 GHz	100W

[*Click here for a full list of supported CPUs](#)

**Preceding CPU Generations and higher TDP CPUs may be supported under certain configurations. Please [contact Trenton Systems](#) for additional information about specialized system optimization.*

MEMORY

Slots: 8x DDR4 with ECC support

Memory Support: Eight channels

Capacity: Up to 1TB DDR4 ECC RDIMM

Type: ECC DDR4-2933 RDIMM

DIMM Sizes: 128GB, 64GB, 32GB, 16GB

Error Detection: Corrects single-bit errors and detects double-bit errors using ECC memory

STORAGE

Type(s):

- ▶ 2x SSD/HDD SATA3 (6 Gbps) drives of any size with Riser
- ▶ 4x M.2 NVMe PCIe 3.0 x4 with Riser

Capacity: No current limit on drive capacity

SATA Modes: AHCI or RAID

RAID: Intel® RST SATA RAID support 0/1/5/10 Modes

PCI SLOT CONFIGURATION

Type(s): x2 PCIe Gen 3 x16 with Riser

ON-BOARD DEVICES

Chipset: Intel® C622

IPMI: Support for Intelligent Platform Management Interface v2

- ▶ IPMI 2.0 with virtual media over LAN and KVM-over-LAN support

Network Controllers:

- ▶ Dual Intel® i350AM2 Gigabit Ethernet
- ▶ Intel® x556 10 Gigabit Ethernet
- ▶ Dual Intel® i210 Gigabit Ethernet

Graphics: ASPEED AST2400 BMC; VGA 1920X1200@60Hz 32bpp

TPM 2.0: Secure cryptoprocessor that helps you with actions such as generating, storing, and limiting the use of cryptographic keys. A requirement for Microsoft's bitlocker drive volume encryption features.

INPUT / OUTPUT

USB: 7x USB 3.0 Ports

- ▶ 3x USB 3.0 Ports on Board
- ▶ 4x USB 3.0 Ports via Midplane and/or Riser

Display: 1x VGA Port

LAN: 6x RJ-45 Ethernet LAN ports

- ▶ 2x RJ-45 10 Gigabit Ethernet LAN Ports
- ▶ 4x RJ-45 Gigabit Ethernet LAN Ports (rear, midplane)
 - 1x i210 Gigabit Ethernet LAN Port
 - 1x i210/IPMI Gigabit Ethernet LAN Port
 - 1x MPI350 Gigabit Ethernet LAN Port
 - 1x MPI350 Gigabit Ethernet LAN Port

Serial: 1x RS232 Serial Port via Header

PROCESSOR BOARD WEIGHT

Average Weight: 6.3 lbs.

**System weight and dimensions dependent on rugged chassis and component selection*

SYSTEM BIOS

BIOS Type: 128Mb Macronix MX25L12835FM2I-10G SPI Serial EEPROM (SPI Flash)

BIOS Features:

- ▶ Plug and Play (PnP)
- ▶ TPM 2.0
- ▶ PCI 2.2
- ▶ ACPI 1.0 / 2.0
- ▶ USB Keyboard Support
- ▶ SMBIOS 2.3
- ▶ UEFI

SYSTEM MANAGEMENT

ASPEED AST2400 Baseband Management Controller: rKVM, System Monitoring, Out of Band Management

ENVIRONMENTAL SPECIFICATIONS

Operating Temperature: 0°C - 50°C

Storage Temperature: -40°C - 70°C

Operating Humidity: 8% - 90% Non-Condensing

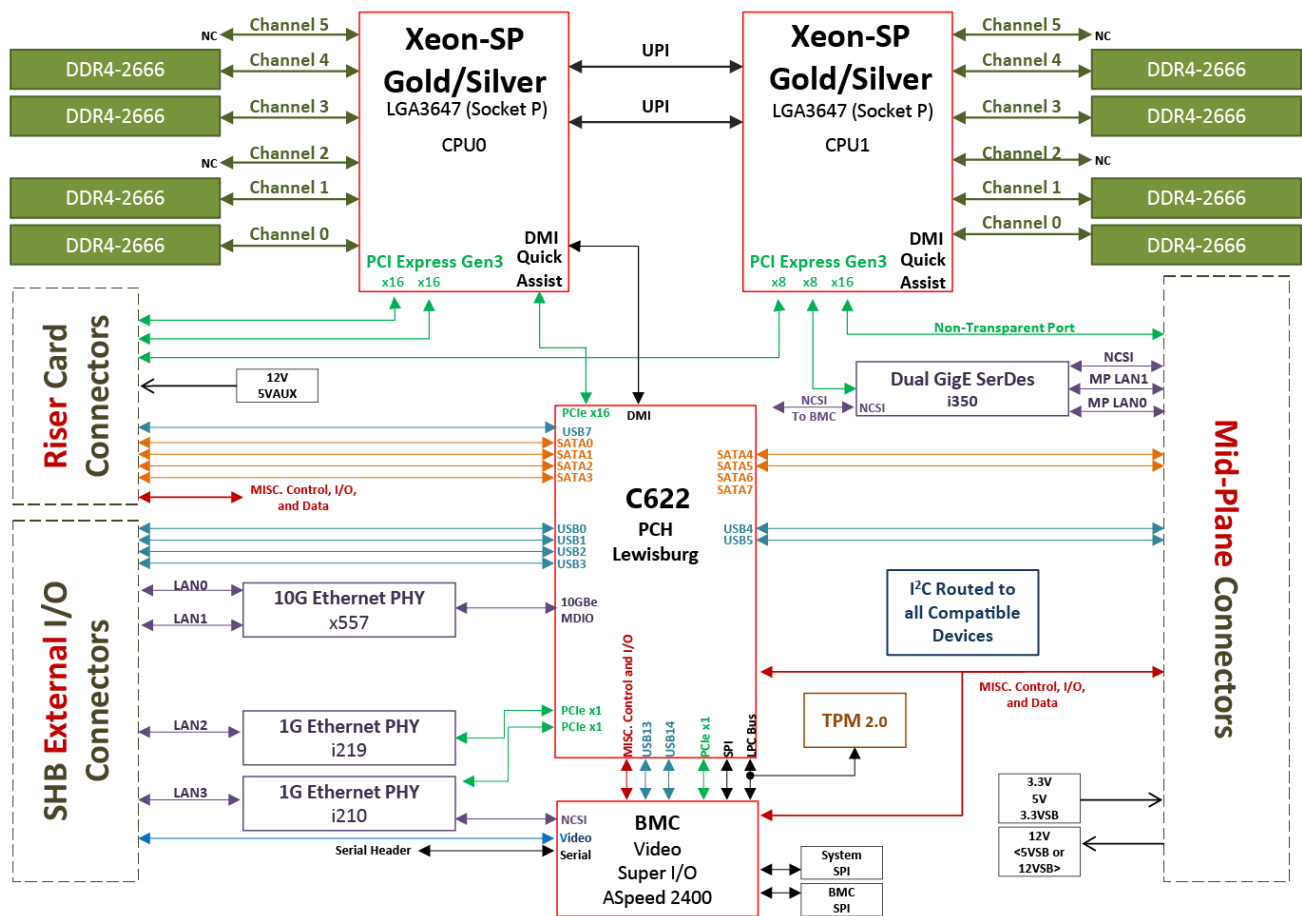
Non-operating Humidity: 5% - 95% Non-Condensing

**Numbers noted are dependent on CPU selection. Please [contact Trenton Systems](#) for specific CPU environmental specs.*

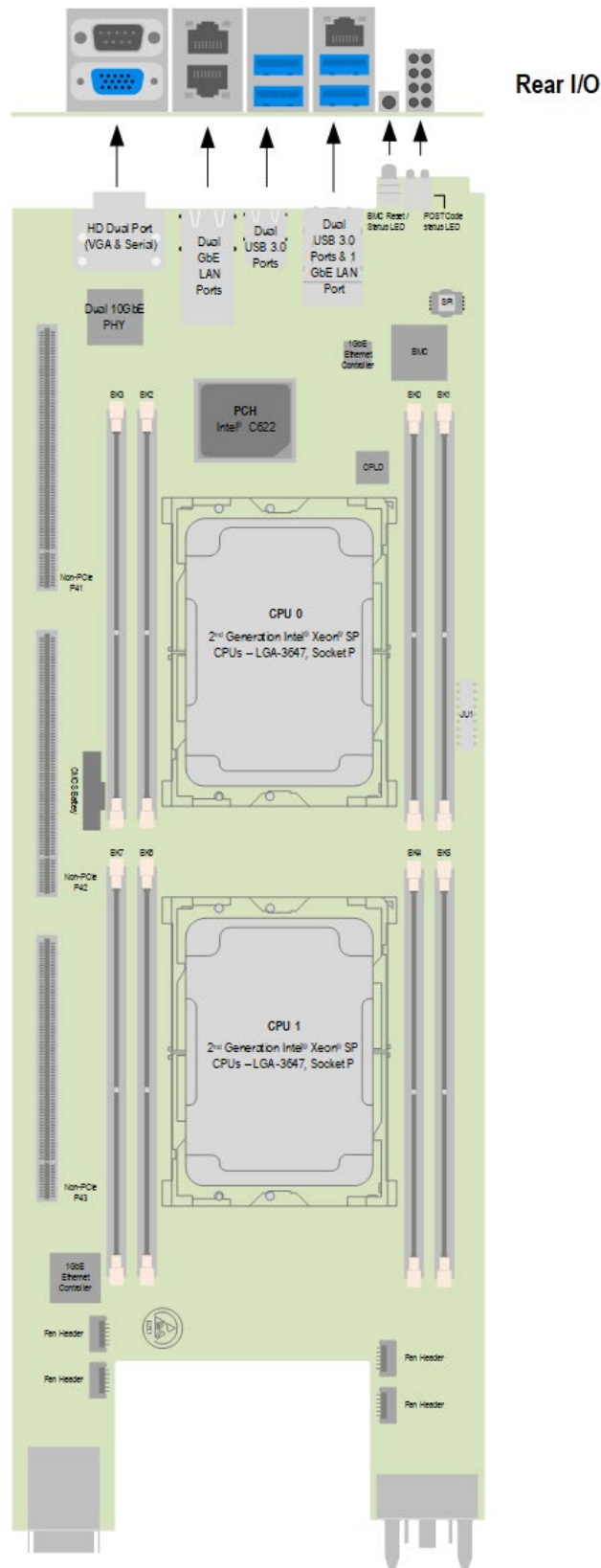


Diagrams & Layouts

BLOCK DIAGRAM



LAYOUT DRAWING



Technical Specifications

PROCESSORS

- ▶ Intel® Xeon® Scalable Processors
- ▶ Processor plugs into an LGA3647 socket

SUPPORTED INTEL® PROCESSOR TECHNOLOGIES

Intel® Deep Learning Boost: This technology enhances the performance of Second-Generation Xeon Scalable processors powering artificial intelligence applications. DL Boost is a relatively new set of embedded processor technologies. By extending Intel's AVX-512 instruction set using a Vector Neural Network Instruction (VNNI) set, DL Boost accelerates AI inference performance, which is how an application's AI algorithm applies logic to produce new information.

Intel® Resource Director Technology: This technology is a framework for resource allocation that consists of five individual technologies: Cache Allocation Technology (CAT), Code and Data Prioritization (CDP), Memory Bandwidth Allocation (MBA), Cache Monitoring Technology (CMT) and Memory Bandwidth Monitoring (MBM). For an overview of each, visit Intel's [RDT resource webpage](#).

Intel® Speed Shift Technology: This technology uses hardware-controlled P-states to deliver quicker responsiveness with single-threaded, short-duration workloads, such as web browsing, by allowing the processor to more quickly select its best operating frequency and voltage for optimal performance and power efficiency.

Intel® Hyper-Threading (Intel® HT): This processor technology allows simultaneous multithreading of CPU tasks to enable parallel system operations. An operating system that is hyper-threading aware can address each core as a logical processor in order to spread out execution tasks to improve application software efficiency and overall system speed.

Intel Virtualization Technology (Intel® VT-x): Enabled in the SHB's BIOS, this technology enables multiple operating systems to run in specific processor cores thereby creating virtual machines (VMs) on a single SHB.

Intel Virtualization Technology for Directed I/O (Intel® VT-d): This is a sub-set of Intel VT-x and enables I/O device assignments to specific processor cores or VMs. Intel VT-d also supports DMA remapping, interrupt remapping and software DMA and interrupt status reporting. Intel VT-d is an optional extension to the Intel VT-x technology.



Intel® VT-x with Extended Page Tables (EPT): This feature is enabled in the Skylake-S microarchitecture to support the processor's "real mode" or unrestricted guest feature.

Intel® vPro: This technology is a set of hardware and security features designed to improve and streamline the performance of business computers and servers. Intel created vPro to deliver benefits across four major areas of computing in business environments: performance, security, manageability and stability. These features include, but are not limited to, technologies such as Intel Optane Memory, Intel Hardware Shield, Trusted Platform Module (TPM) 2.0 and Intel Active Management (AMT) Technology.

Intel® Transactional Synchronization Extensions: This processor technology is an addition to Intel's x86 instruction set architecture. It adds support for hardware transactional memory to improve the performance of multi-threaded applications. The technology was introduced with Intel's Fourth-Generation Core Processors and is utilized by Xeon processors as well.

Intel® Trusted Execution Technology (Intel® TXT): This feature is a security technology designed to address software attacks at the hardware level. It uses a software verification process called Measured Launch Environment (MLE) as well as boot process isolation for added security.

Intel® Turbo Boost Technology 2.0: The higher performance Skylake-S processors may run above the processors stated clock speed via a new dynamic processor speed control technology called Intel Turbo Boost 2.0. The processor enters the boost mode when the operating system requests the highest possible performance state as defined by the Advanced Configuration and Power Interface or ACPI.

Intel® 64: This technology is Intel's 64-bit computing upgrade to its 32-bit x86 instruction set architecture. A 64-bit Xeon processor improves multitasking and supports larger file sizes through its improved support of data allocation. The architecture itself allows systems to address up to 1TB of memory when combined with the appropriate 64-bit operating system.

Intel® Instruction Set Extensions: This technology is a collection of additional instructions, such as Intel SSE4.2 and Intel AVX, used to boost the performance of a CPU.

Intel® Advanced Encryption Standard New Instructions (Intel® AES-NI): Seven new instructions available in the Skylake-S micro-architecture makes pervasive encryption in an IT environment possible while enabling implementation that is faster and more affordable by providing advanced data protection and greater hardware platform security.

Intel® Enhanced SpeedStep Technology: This technology is centered around the management of power consumption and heat production. It's a two-fold solution for delivering high performance to mobile computing systems while also saving power. It does so via an automatic,



separatory adjustment of CPU voltage and core frequency, as well as through clock partitioning and recovery.

Intel® Volume Management Device: This technology addresses hot-swappable storage and storage management. The technology allows for the removal and subsequent service of PCIe-based NVMe SSDs without the powering down of the server or workstation. The main goal of Intel VMD is to improve uptime and serviceability for servers and workstations.

Intel® Execute Disable Bit: This feature is a hardware-based technology that helps protect systems from viruses and malicious code. EDB enables the CPU to label which areas of memory can and cannot execute application code, thereby stopping computer worms and viruses as they attempt to execute their own code during a buffer overflow attack.

Intel® Run Sure Technology: This technology provides additional reliability, availability and serviceability (RAS) features, and memory error corrections, that help increase server uptime and protect critical data. It combines a server's processor, firmware and software resources to help diagnose errors, automatically recover data and ensure data integrity within the memory subsystem.

Intel® Mode-Based Execute Control: This technology is a security enhancement of Extended Page Tables that functions as an additional safeguard against malware attacks. MBE provides an extra layer of protection from malware attacks in a virtualized environment by enabling hypervisors to more reliably verify and enforce the integrity of kernel-level code.

SERIAL INTERCONNECT INTERFACE

PCI Express® 3.0, 2.0, and 1.1 compatible.

SERIAL INTERCONNECT SPEEDS

- ▶ PCI Express 3.0 – 8.0GHz per lane
- ▶ PCI Express 2.0 – 5.0GHz per lane
- ▶ PCI Express 1.1 - 2.5GHz per lane

PLATFORM CONTROLLER HUB (PCH)

- ▶ Intel® C622 Platform Controller Hub (Lewisburg)

MEMORY INTERFACE

The MSL8256 features eight memory channels of DDR4 with one RDIMM per channel for a maximum of 1TB of memory. These DDR4-2666 memory interface channels support up to eight ECC PC4-21300 standard memory RDIMMs. Non-ECC DDR4 RDIMMs are also supported, but the



two memory types cannot be used together on the processor board. The peak memory interface transfer rate per channel is 2666MT/s when using PC4-21300 DIMMs.

The System BIOS automatically detects memory type, size and speed. Trenton Systems recommends ECC PC4-21300 DDR4 RDIMM memory modules for use on the MSL8256. These ECC (64-bit) DDR4 DIMMs must be PC4-21300 compliant.

INTERRUPTS

The processor board is fully PC-compatible with interrupt steering for PCI plug and play compatibility.

BIOS (FLASH)

The MSL8256 board uses an Aptio® 5.x BIOS from American Megatrends Inc. (AMI). The BIOS features built-in advanced CMOS setup for system parameters, peripheral management for configuring on-board peripherals and other system parameters. The BIOS resides in a 128Mb Macronix MX25L12835FM2I-10G SPI Serial EEPROM (SPI Flash). Custom BIOSes are available.

CACHE MEMORY

The processors include either a 4MB, 6MB or 8MB Intel® Smart Cache memory capacity that is equally shared between all of the processor cores on the die.

ETHERNET INTERFACES

The MSL8256 supports five Ethernet interfaces. The first two interfaces are on-board 10/100/1000 Base-T Ethernet interfaces located on the board's I/O bracket and implemented using a Dual Intel® i350 Dual Gigabit Ethernet Controller. These I/O bracket interfaces support Gigabit, 100Base-T and 10Base-TX Fast Ethernet modes and are compliant with the IEEE 802.3 Specification.

The main components of the Ethernet interfaces are:

- ▶ Dual Intel® i350AM2 for 10/100/1000-Mb/s Ethernet.
- ▶ Dual Intel® i210 for 10/100/1000-Mb/s Ethernet.
- ▶ Intel® x556 10 Gigabit Ethernet for 10,000 Mb/s Ethernet.
- ▶ Integrated RJ-45/Magnetics module connectors on the processor board's I/O bracket for direct connection to the network. The connectors require category 5 (CAT5) unshielded twisted-pair (UTP) 2-pair cables for a 100-Mb/s network connection or category3 (CAT3) or higher UTP 2-pair cables for a 10-Mb/s network connection. Category 5e (CAT5e) or higher UTP 2-pair cables are recommended for a 1000-Mb/s (Gigabit) network connection.
- ▶ Link status and activity LEDs on the I/O bracket for status indication (See Ethernet LEDs and Connectors later in this chapter.)



TRUSTED PLATFORM MODULE 2.0

The MSL8256 provides support for Trusted Platform Module 2.0 operations via an Infineon SLB9665 controller. This feature aids in assuring platform integrity by providing a system designer the capability to form a root of trust in conjunction with the BIOS and system firmware.

WATCHDOG TIMER (WDT)

The MSL8256 provides a programmable watchdog timer with programmable timeout periods of 1 msec to 1 minute. When enabled, the WDT will generate a system reset. WDT control is supplied via the General Purpose IO pins from the Intel® C622 Platform Controller Hub (PCH). The PCH's WDT_x GPIO signals are:

- ▶ WDT_TRIG – GPP_A23
- ▶ WDT_SEL2 – GPP_K2
- ▶ WDT_SEL1 – GPP_K1
- ▶ WDT_SELO – GPP_K0

As soon as the select lines are set to not-disabled, software needs to toggle the trigger within the timeout period, or a reset occurs.

Watchdog Timeout Period Selection:

WATCH DOG TIMER INTERVALS			
GPP_K2 WDTSEL2	GPP_K1 WDTSEL1	APP_K0 WDTSELO	WDT TIMEOUT PERIOD
0	0	0	1msec
0	0	1	10msec
0	1	0	30msec
0	1	1	WDT DISABLED (default)
1	0	0	100msec
1	0	1	1sec
1	1	0	10sec
1	1	1	1min

POWER REQUIREMENTS

Actual power number will vary as a function of system application. Contact Trenton Systems for application-specific power figures.

BATTERY

A replaceable Panasonic lithium coin cell CR2032 battery is provided for ten years of data retention for CMOS memory.



CAUTION: There is a danger of explosion if the battery is incorrectly replaced. Replace it only with the same or equivalent type recommended by the battery manufacturer. Dispose of used batteries according to the battery manufacturer’s instructions.

TEMPERATURE/ENVIRONMENT

TYPE	DESCRIPTION
Operating Temperature	0° C. to 45° C for all CPU options
Air Flow Requirement	350LFM continuous airflow
Storage Temperature	- 40°C to 70°C
Humidity	5% to 90% non-condensing

INDUSTRY CERTIFICATIONS

This processor board is designed to meet a variety of internationally recognized industry standards including UL60950, CAN/CSA C22.2 No. 60950-00, EN55022:1998 Class B, EN6100-4-2:1995, EN61000-4-3:1997, EN61000-4-4:1995, EN61000-4-5:1995, EN61000-4-6:1996 and EN61000-4-11:1994.

CONFIGURATION JUMPERS

The setup of the configuration jumpers on the processor board is described below. An asterisk (*) indicates the default value of each jumper.

NOTE: Jumper JU1 is a dual-row, 16-pin jumper. Each position controls the operation of a specific SHB implementation.

PINS	PURPOSE
1-2	Install on pins 1 and 2 for normal operation
3-4	To clear CMOS: Remove and drain AC power. Move the shunt on PINs 1: 2 to 3:4 for a couple of seconds. Return the shunt from PINs 3:4 back to 1:2. Apply AC power and permit the system to land on the first boot device. The system will cycle power 2-3 times as part of this procedure, so do not be alarmed.
JU1 PINs 7:8	Password clear. For use: Drain AC power. Install a shunt on PINs 7:8 and boot to first boot device. Drain AC power, remove this shunt and boot as normal.
11-12	Flash security override

STATUS LEDs



POST Code LEDs 1 – 8

As the POST (Power On Self-Test) routines are performed during boot-up, test codes are displayed on Port 80 POST Code LEDs 0, 1, 2, 3, 4, 5, 6 and 7. These LEDs are located on the rear I/O panel of the module.

These POST codes may be helpful as a diagnostic tool. Specific test codes are listed in Appendix A - BIOS Messages section of the MSL8256 Technical Reference Manual. After a normal POST sequence, the LEDs are off (00h) indicating that the processor board’s BIOS has passed control over to the operating system loader typically at interrupt INT19h. The chart is from Appendix A and can be used to interpret the LEDs into hexadecimal format during POST.

P4A/P4B ETHERNET LEDS

The I/O bracket houses the three RJ-45 network connectors for Ethernet LAN1, LAN2, and LAN3. Each LAN interface connector has two LEDs that indicate activity status and Ethernet connection speed. Listed below are the possible LED conditions and status indications for each LAN connector:

LED/CONNECTOR	DESCRIPTION
Activity LED	This LED identifies the validity of a link on the specific interface. This is the upper LED on the LAN connector (i.e., toward the upper memory sockets).
Off	No valid link exists on this interface.
On (flashing)	Indicates network transmit or receive activity.
On (solid)	Indicates a valid link with no transmit or receive activity.
Speed LED	This multi-color LED identifies the connection speed of the SHB’s P4A (LAN2) and P4B (LAN1) Ethernet interfaces. These are the lower LEDs on the dual LAN connector (i.e., toward the edge connectors).
Green	Indicates a valid link at 1000-Mb/s or 1Gb/s
Orange	Indicates a valid link at 100-Mb/s.
Off	Indicates a valid link at 10-Mb/s
RJ-45 Network Connectors	The RJ-45 network connector requires a Connector category 5 (CAT5) unshielded twisted-pair (UTP) 2-pair cable for a 100-Mb/s network connection or a category 3 (CAT3) or higher UTP 2-pair cable for a 10-Mb/s network connection. A category 5e (CAT5e) or higher UTP 2-pair cable is recommended for a 1000-Mb/s (Gigabit) network connection.



SYSTEM BIOS SETUP UTILITY

The MSL8256 features the Aptio® BIOS from American Megatrends, Inc. (AMI) with a ROM-resident setup utility called the Aptio Text Setup Environment or TSE. The TSE setup utility allows you to select to the following categories of options:

- ▶ Main Menu
- ▶ Advanced Setup
- ▶ Boot Setup
- ▶ Security Setup
- ▶ Chipset Setup
- ▶ Exit

Each of these options allows you to review and/or change various setup features of your system. Contact Trenton for application-specific BIOS information and support.

Trenton Systems is attaching a copy of American Megatrends Aptio 5.x Status Codes in this manual for your reference. This is a public document and the latest version can be downloaded at [https://ami.com/ami_downloads/Aptio V Status Codes.pdf](https://ami.com/ami_downloads/Aptio_V_Status_Codes.pdf).



Trenton Systems
1725 MacLeod Drive
Lawrenceville, GA 30043

www.trentonsystems.com
t. 770.287.3100
e. info@trentonsystems.com

