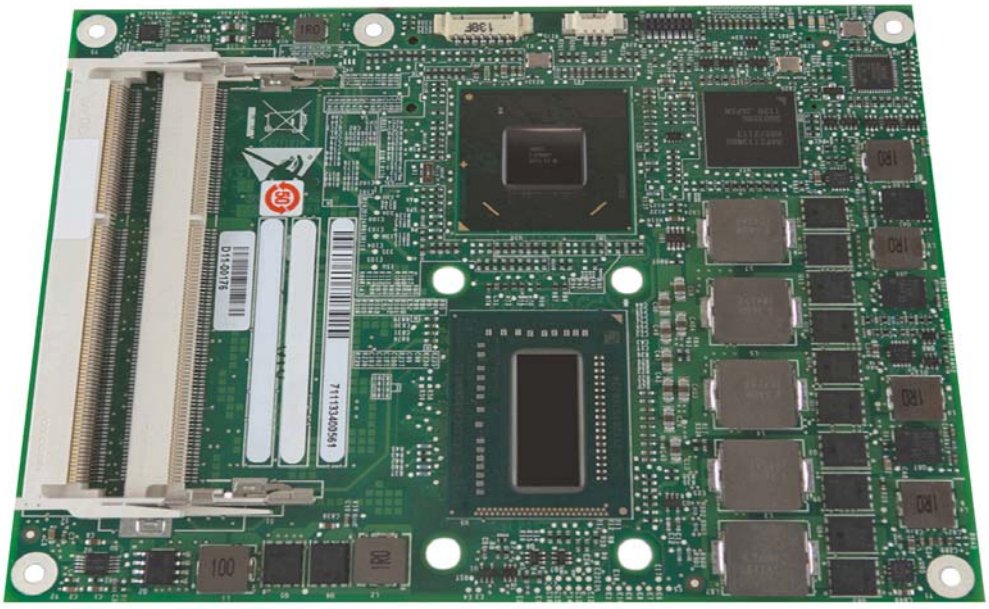
Product Manual

radisys



COM EXPRESS®

CEQM77

June 2012 **007-03494-0000**

Revision history

Version	Date	Description
-0000	June 2012	First edition.

Table of Contents

Table of Contents

Table of Contents

Table of Contents

Preface

About this manual

This manual is written primarily for system engineers who will integrate the Radisys® CEQM77 COM Express® embedded computing module into a compatible COM Express carrier board. In this manual the CEQM77 COM Express module will be referred to as the "COM Express module."

See the following resources for information on the COM Express module not described in this manual:

- **Installation and initial setup instructions.** The *CEQM77 COM Express Module Quick Start Guide* provides steps for assembling a COM Express system.

  When referenced in this manual, the simplified name of *Quick Start Guide* will be used.
- **BIOS configuration information.** The *CEQM77 System Setup Utility Specification* describes the system setup utility interfaces and configuration options.

  When referenced in this manual, the simplified name of *System Setup Utility Specification* will be used.
- **Carrier design guidelines and thermal validation procedures.** The *COM Express Design Guidelines* supplements the *PICMG® COM Express Carrier Design Guide,* and describes special considerations and guidelines for designing a carrier board to use with the COM Express module.

  When referenced in this manual, the simplified name of *COM Express Design Guidelines* will be used.
- **List of approved components.** The *CEQM77 COM Express Module Approved Components List* identifies the DDR3 SDRAMs, SSDDR modules, and other external components and devices that Radisys has validated for use with the COM Express module.

  When referenced in this manual, the simplified name of *Approved Components List* will be used.
- **Firmware and software update information.** Updates for the BIOS, embedded controller firmware, and drivers may be available for the COM Express module from time to time. Detailed procedures on updating the firmware and software are included in the corresponding release packages.

Electrostatic discharge

WARNING! This product contains static-sensitive components and should be handled with care. Failure to employ adequate anti-static measures can cause irreparable damage to components.

Electrostatic discharge (ESD) damage can result in partial or complete device failure, performance degradation, or reduced operating life. To avoid ESD damage, the following precautions are strongly recommended.

- Keep each board in its ESD shielding bag until you are ready to install it.
- Before touching a board, attach an ESD wrist strap to your wrist and connect its other end to a known ground.
- Handle the board only in an area that has its working surfaces, floor coverings, and chairs connected to a known ground.
- Hold boards only by their edges and mounting hardware. Avoid touching PCB components and connector pins.

For further information on ESD, visit www.esda.org.

Where to get more product information

Visit the Radisys web site at www.radisys.com for product information and other resources. Downloads (manuals, release notes, software, etc.) are available at www.radisys.com/downloads.

Chapter 1

Product Overview

The COM Express modules described in this manual are compliant with *PICMG® COM.0 COM Express Module Base Specification Revision 2.0* and use Type 6 pinouts. These COM Express modules are based on the Intel® Chief River platform and fit in the COM Express basic form factor. Feature highlights include:

- Intel Ivy Bridge processor for
  - larger L2 and L3 caches
  - micro-architecture improvements
  - faster memory speeds
  - DDR3 memory
  - improved graphics performance
- Intel Panther Point platform controller hub (PCH) chipset
- Modular design for reuse, interchangeability, and rapid design updates to meet market changes, demand fluctuations, and performance upgrades
- Additional feature highlights:
  - Premium PCI Express Graphics (PEG) or standard integrated graphics support
  - Trusted Platform Management (TPM)
  - Support for Intel Management Engine (ME) power states M0, M3, and M_{off} (optional)
  - One fan tach input signal and one PWM output signal
  - Legacy device support by managing appropriate LPC Super I/O chips
  - Extensive I/Os
  - BIOS readiness for legacy and EFI native operating systems
  - Micro-SD socket (optional)
  - Second BIOS SPI flash (optional)
  - SSDDR3 support (optional)

COM Express product codes

COM Express modules

Table 1 lists the modules available at the time of production release. All modules are RoHS-, EN-, FCC-, IEC-, and UL-compliant.

CEQM77 “C-Temp” (commercial temperature) modules operate in ambient temperatures ranging from 0°C to +60°C.

Table 1. COM Express module product codes

Model	Product code	Intel Calpella platform	TPM	AMT	Pinout
C-Temp	CEQM77-3612-0	• Intel Core i7-3612QE processor, 2.1GHz, quad-core • Intel QM77 PCH chipset	Yes	Yes	Type 6
	CEQM77-3615-0	• Intel Core i5-3615QE processor, 2.3GHz, quad-core • Intel QM77 PCH chipset	Yes	Yes	Type 6
	CEQM77-3517-0	• Intel Core i7-3517UE processor, 1.7GHz, dual-core • Intel QM77 PCH chipset	Yes	Yes	Type 6
	CEQM77-3555-0	• Intel Core i7-3555LE processor, 2.5GHz, dual-core • Intel QM77 PCH chipset	Yes	Yes	Type 6
	CEQM77-3610-0	• Intel Core i5-3610ME processor, 2.7GHz, dual-core • Intel QM77 PCH chipset	Yes	Yes	Type 6

Thermal solutions

Radisys offers two types of RoHS-compliant thermal solutions, the CEQM67-AHS active heatsink and the CEQM67-77-HSP heat spreader. See *Chapter 4, Thermal Solutions, on page 59* for detailed information about these thermal solutions.

Module layout

CEQM77

Figure 1. Module layout: top view

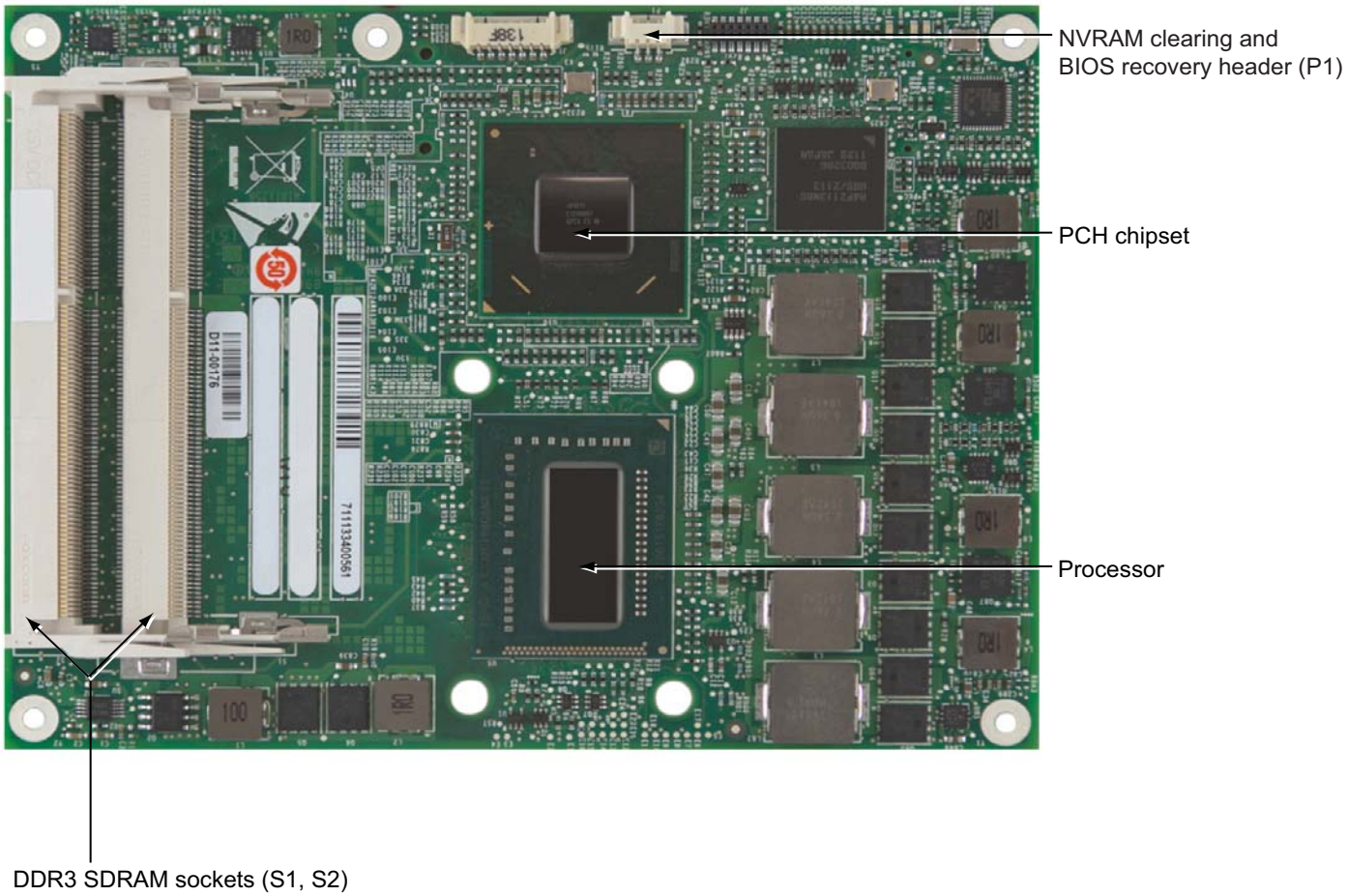
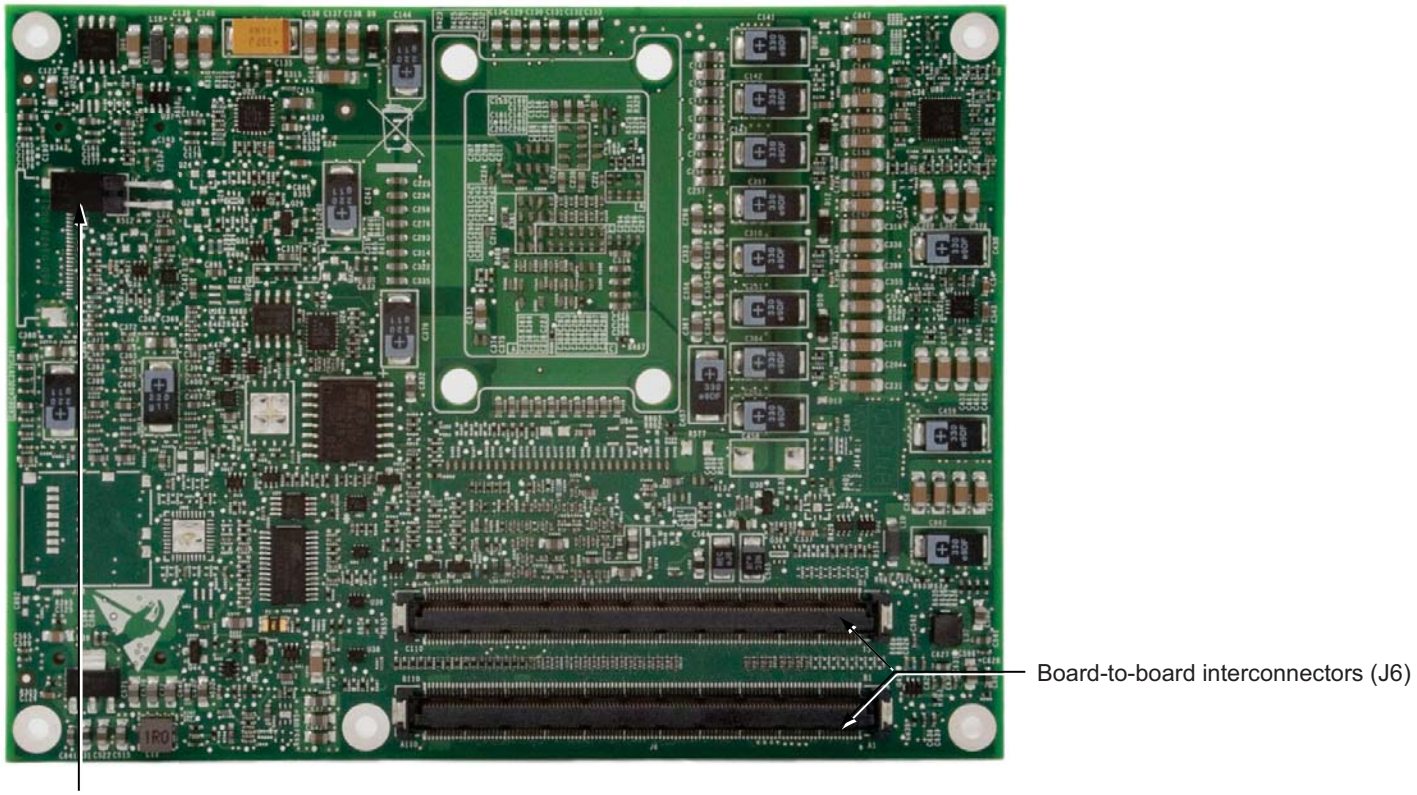


Figure 2. Module layout: bottom view



Product Specifications

Mechanical specifications

The PCB size of the COM Express module conforms to the basic form factor defined in the PICMG specification: 125mm x 95mm.

Table 2. PCB measurements

Measurement	Size/location (mm)	Tolerance (mm)
PCB length x width	125 x 95	±0.25mm
PCB thickness	2.18	±0.22mm
Board-to-board interconnector peg hole locations	[16.50, 6.00] and [16.50, 18.00]	±0.10mm

Figure 3. Basic module size form factor (in millimeters)

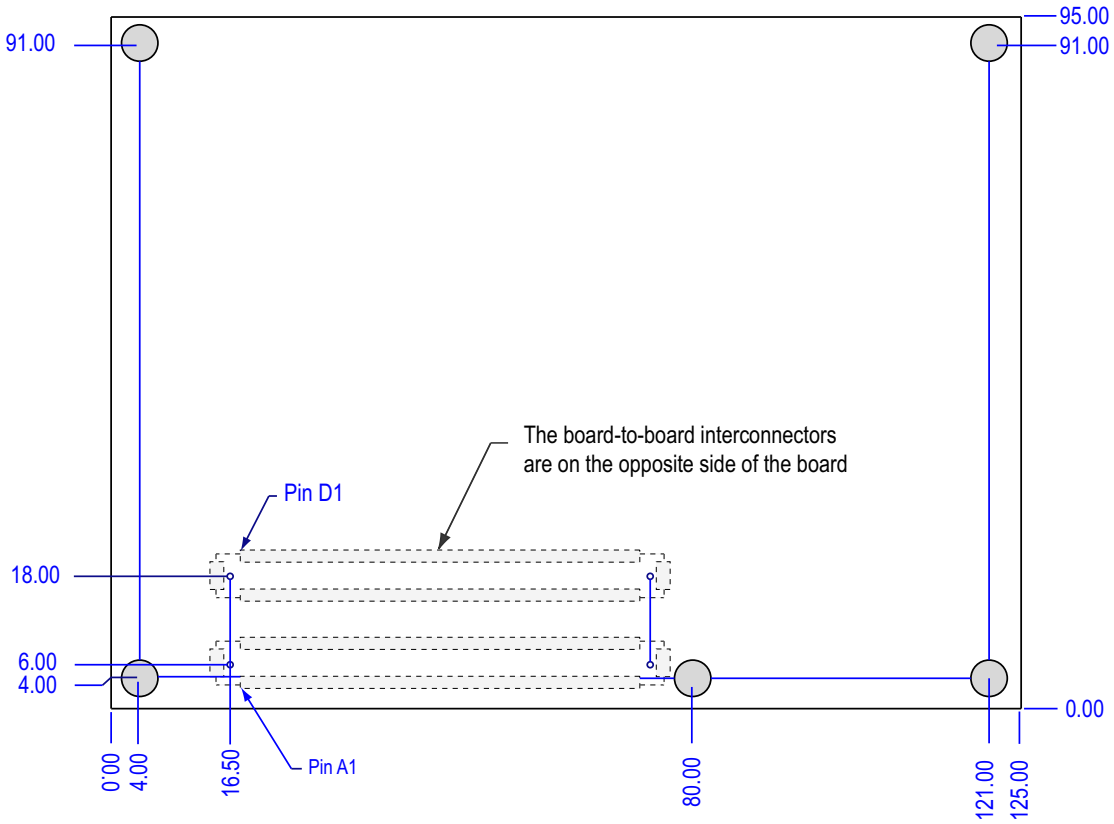


Figure 4. Module envelope dimensions (mm): top view

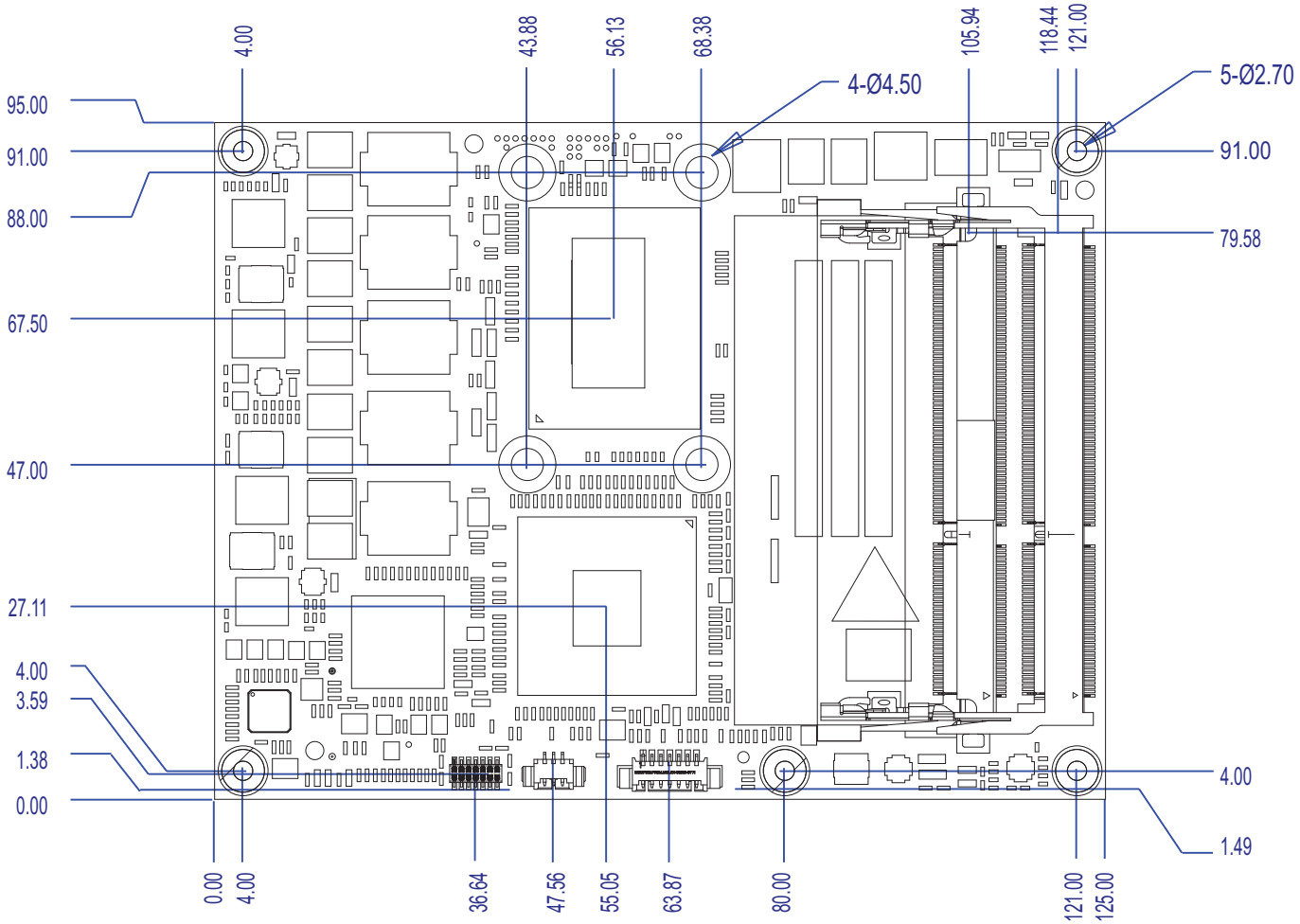


Figure 5. Module PCB height (mm)

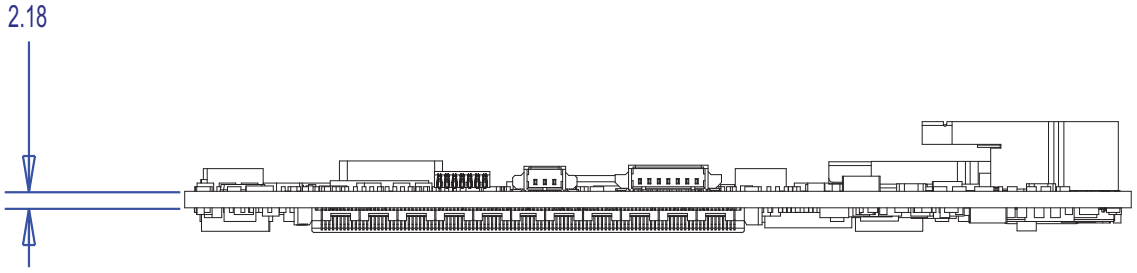
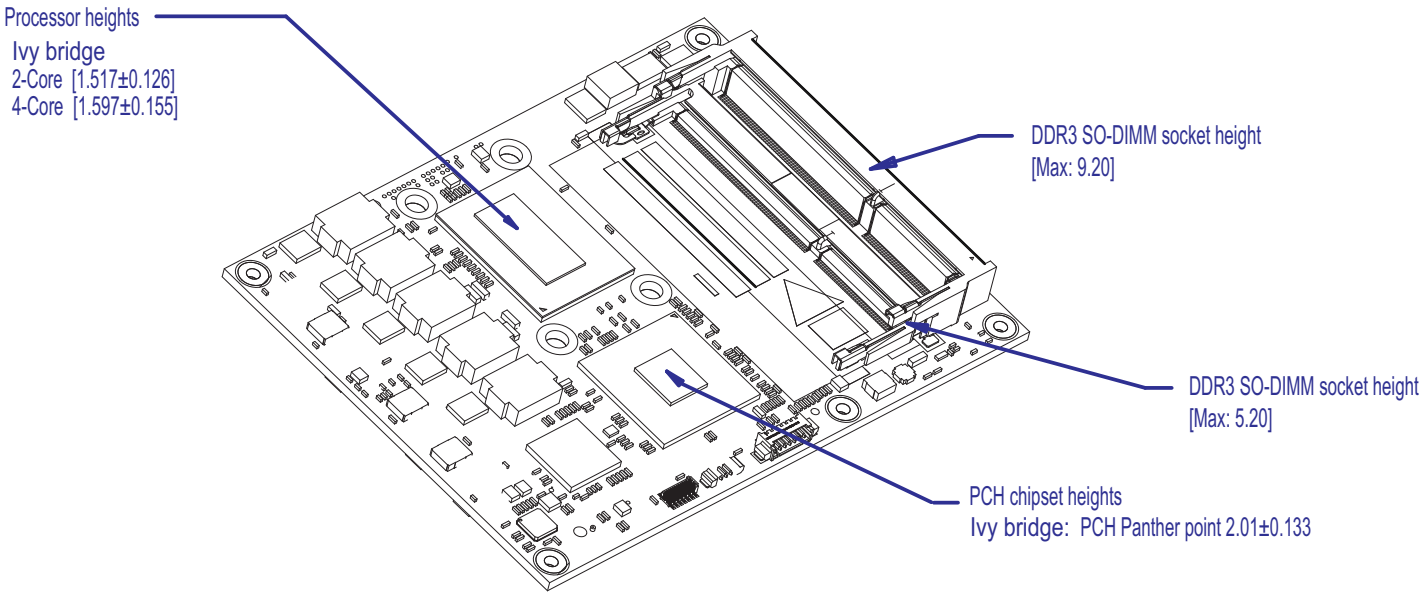


Figure 6. Module component dimensions (mm)



Module interconnectors

The board-to-board interconnectors (J6) on the COM Express module use a PICMG-compliant 440-pin receptacle connector (part number: AMP/Tyco 3-1827231-6), comprising two 220-pin, 0.5mm pitch receptacles.

For pinout definitions of the board-to-board interconnectors and required/optional features for the corresponding COM Express pinout type, see *COM Express Module Pinout Definitions on page 71*.

Stack-up heights

Height constraints when used with a CR300 carrier board

The COM Express module, together with a Radisys active heatsink and carrier board, requires a chassis with a minimum height of two rack mount units (2U = 88.90mm = 3.50 inches).

Figure 7 on page 16 illustrates the height constraints of a COM Express assembly, where the heat spreader is only used as an interface for custom thermal solutions. An explanation of each height constraint is given in the table below the figure.

Figure 7. Height constraints of a typical system

Item	Height constraints
A	Parts mounted on the top side of the module's PCB have a maximum height of 6mm with the exception of the 9.2mm DDR3 SDRAM socket.
B	Parts mounted on the bottom side of the module's PCB have a maximum height of 3.8mm. This affects the maximum allowable height of carrier board components underneath the module. • The board-to-board interconnectors on the CR300 carrier board are 8mm in height, so the clearance between the carrier board and the bottom surface of the module's PCB is 8mm. This allows the use of carrier board components up to 4mm in height underneath the module. • If the board-to-board interconnectors on your custom carrier board has a height of 5mm, the clearance between the carrier board and the bottom surface of the module's PCB is 5mm. This limits the height of carrier board components underneath the module to 1mm.
C	The module's PCB thickness is 2.18mm.
D	The height from the bottom side of the module's PCB to the top side of the heat spreader is 13mm.
E	The stack-up height from the CR300 carrier board PCB to the bottom side of the module's PCB is 8mm. A custom carrier board may have a stack-up height of 5mm.
F	The COM Express module with the Radisys thermal solution and carrier board fits in a 2U chassis (88.90mm).

Electrical specifications

Module power consumption

The amount of power consumed by the COM Express modules is highly dependent on the processor, memory, attached devices, software in use, and power state. The module power consumption is tested with the following system configuration:

- Carrier board: CR300 ATX carrier board
- Memory: Micron®, MT16JTF1G64HZ-1G6D1, 8GBx2
- Hard disk: HITACHI® HDS728080PLA380 80GB
- Monitor: Samsung® SyncMaster743n
- Keyboard and mouse: Viewsonic®, VS10230, USB
- ATX PSU: SPI® SPI350PFB
- Operating system: Microsoft Windows 7 (64bit)
- Test software: TAT4.x, Prime95, 3DMark11

Table 3. CEQM77-3612-0 module power rail current consumption

Main rail current consumption	Current (A) at +12V	Current (A) at +5V standby	Total power consumption (W)
At Windows Desktop Idle	1.070	0.080	13.032
Running System Stress (Prime95: Blend)	5.370	0.080	63.235
Running System Stress (Prime95: In-place Large FFTs)	5.400	0.080	63.586
Running System Stress (Prime95: Small FFTs + 3DMark11)	5.300	0.090	62.467
Running Windows Stress (3DMark11)	3.200	0.080	37.846
In standby mode S3	0.000	0.160	0.813
In hibernation mode S4	0.000	0.014	0.071
In power off mode S5	0.000	0.014	0.071

Table 4. CEQM77-3615-0 module power rail current consumption

Main rail current consumption	Current (A) at +12V	Current (A) at +5V standby	Total power consumption (W)
At Windows Desktop Idle	1.060	0.080	12.914
Running System Stress (Prime95: Blend)	5.800	0.081	68.271
Running System Stress (Prime95: In-place Large FFTs)	5.820	0.081	68.505
Running System Stress (Prime95: Small FFTs + 3DMark11)	6.400	0.097	75.373
Running Windows Stress (3DMark11)	3.100	0.080	36.676
In standby mode S3	0.000	0.160	0.813
In hibernation mode S4	0.000	0.012	0.061
In power off mode S5	0.000	0.012	0.061

Table 5. CEQM77-3517-0 module power rail current consumption

Main rail current consumption	Current (A) at +12V	Current (A) at +5V standby	Total power consumption (W)
At Windows Desktop Idle	1.069	0.036	12.797
Running System Stress (Prime95: Blend)	3.066	0.058	36.167
Running System Stress (Prime95: In-place Large FFTs)	2.980	0.058	35.161
Running System Stress (Prime95: Small FFTs + 3DMark11)	3.480	0.076	41.102
Running Windows Stress (3DMark11)	3.000	0.073	35.471
In standby mode S3	0.000	0.160	0.813
In hibernation mode S4	0.000	0.014	0.071
In power off mode S5	0.000	0.014	0.071

Table 6. CEQM77-3555-0 module power rail current consumption

Main rail current consumption	Current (A) at +12V	Current (A) at +5V standby	Total power consumption (W)
At Windows Desktop Idle	1.050	0.040	12.593
Running System Stress (Prime95: Blend)	3.550	0.070	41.891
Running System Stress (Prime95: In-place Large FFTs)	3.520	0.070	41.540
Running System Stress (Prime95: Small FFTs + 3DMark11)	4.650	0.070	54.761
Running Windows Stress (3DMark11)	3.200	0.067	37.778
In standby mode S3	0.000	0.155	0.787
In hibernation mode S4	0.000	0.014	0.071
In power off mode S5	0.000	0.014	0.071

Table 7. CEQM77-3610-0 module power rail current consumption

Main rail current consumption	Current (A) at +12V	Current (A) at +5V standby	Total power consumption (W)
At Windows Desktop Idle	1.090	0.036	13.045
Running System Stress (Prime95: Blend)	3.600	0.086	42.557
Running System Stress (Prime95: In-place Large FFTs)	3.560	0.086	42.089
Running System Stress (Prime95: Small FFTs + 3DMark11)	5.200	0.094	61.318
Running Windows Stress (3DMark11)	3.150	0.086	37.292
In standby mode S3	0.000	0.160	0.813
In hibernation mode S4	0.000	0.014	0.071
In power off mode S5	0.000	0.014	0.071

Table 8. RTC battery current consumption at G3 (Mechanical Off) state

RTC battery current consumption		Voltage (V)	Current (uA)
Specification	Min	2.000	—
	Max	3.600	6.000
Room temperature, no AC power supply		2.954	2.500

General Purpose I/O (GPIO) power consumption

Table 9 and Table 10 show the GPIO input and output power for the COM Express module:

- GPIO input power consumption
  - V_{IH}: Input High Voltage
  - V_{IL}: Input Low Voltage
- GPIO output power consumption
  - V_{OH}: Output High Voltage
  - V_{OL}: Output Low Voltage
  - I_{OL}: Output Low Current
  - I_{OH}: Output High Current

Table 9. GPIO input

GPIO name	Type	V_{IH}		V_{IL}	
		Min	Max	Min	Max
GPI0	Input	2.0V	3.6V	–0.5V	0.8V
GPI1	Input	2.0V	3.6V	–0.5V	0.8V
GPI2	Input	2.0V	3.6V	–0.5V	0.8V
GPI3	Input	2.0V	3.6V	–0.5V	0.8V

Table 10. GPIO output

GPIO name	Type	V_{OH} (Min)	V_{OL} (Max)	I_{OL}/I_{OH}
GPO0	Output	2.4V	0.44V	12mA/–12mA
GPO1	Output	2.4V	0.44V	12mA/–12mA
GPO2	Output	2.4V	0.44V	12mA/–12mA
GPO3	Output	2.4V	0.44V	12mA/–12mA

Thermal specifications

Table 11 shows the thermal design power (TDP) of the main thermal sources. Note that the TDP specification is used to design the processor thermal solution. The TDP is not the maximum theoretical power the processor can dissipate.

Table 11. TDP of main thermal sources for CEQM77 modules

Component		TDP
Processor	Intel Core i7-3612QE	35W
	Intel Core i7-3615QE	45W
	Intel Core i7-3517UE	17W
	Intel Core i7-3555LE	25W
	Intel Core i5-3610ME	35W
PCH chipset		4.1W
Memory: 4GB, DDR3-1600 MT/s		8W
Gigabit Ethernet controller		1W
CPU VR (75%)	Intel Core i7-3615QE	15W
	Intel Core i7-3612QE	11.7W
	Intel Core i7-3555LE	8.3W
	Intel Core i7-3517UE	5.7W
	Intel Core i5-3610ME	11.7W
Memory VR (75%)		5W
Others		3W

Table 12 shows the thermal limits of the main component junctions.

Table 12. Component temperature limits

Component	Temperature limits	Description
Processor	105°C	Junction temperature
PCH chipset	108°C	Junction temperature
Memory: 4GB, DDR3-1600 MT/s	85°C for C-Temp	Case temperature
Gigabit Ethernet controller	115°C	Junction temperature
CPU VR	150°C	Junction temperature

Note: The local ambient temperature must be within the commercial temperature (C-Temp) range of 0°C to +60°C.

Environmental specifications

The COM Express module meets the following environmental specifications, as tested in a representative system with 4GB of DDR3-1333 SDRAM memory installed.

Performance may vary according to the system it is installed in and environmental conditions. It is particularly important to provide sufficient airflow across the COM Express module to keep its temperature within the specified operating range.

Table 13. CEQM77 environmental specifications (C-Temp)

Characteristic	State	Value
Temperature (board local ambient)	Operating	0° C to +60° C, derated 1.1°C per 305m over 2300m
	Storage (packaged)	–40° C to +85° C
Relative humidity	Operating	5% to 95% RH non-condensing 95% RH at +30°C, linearly derated to 25% RH at +60°C
	Storage (packaged)	5% to 95% RH non-condensing
Altitude	Operating	Up to 4570 meters
	Storage (packaged)	Up to 12000 meters
Shock (drop)	Operating	30G, half sine, 11ms duration, 3 times per face
	Non-operating (unpackaged)	40G, half sine, 11ms duration, 3 times per face
Vibration	Operating	Random 5Hz–2KHz, 7.7grms, 10 minutes in each of 3 axes 5 – 20Hz: 0.004g^2/Hz ramping up to 0.04g^2/Hz 20 – 1000Hz: 0.04g^2/Hz 1000 – 2000Hz: 0.04g^2/Hz ramping down to 0.01g^2/Hz
	Non-operating (unpackaged)	Random 5Hz – 2KHz, 9.7grms, 1hour in each of 3 axes 5 – 20Hz: 0.006g^2/Hz ramping up to 0.06g^2/Hz 20 – 1000Hz: 0.06g^2/Hz 1000 – 2000Hz: 0.06g^2/Hz ramping down to 0.02g^2/Hz Swept sine vibration: 5 – 500Hz, 5g pk-pk, 25.4 mm maximum displacement, 5 minutes dwell at 3 resonance points

Regulatory compliance

EMC compliance

When correctly installed in a suitable chassis, the COM Express module meets these EMC regulations:

- EN55022: 2006+A1
- EN55024: 1998+A1+A2
- FCC Part 15, Subpart B, Class B

Safety compliance

When correctly installed in a suitable chassis, the COM Express module meets these safety regulations:

- UL60950
- EN60950
- IEC60950

Industry compliance

The COM Express module meets these industry standards:

- IPC-6016 (HDI standard)
- European RoHS Directive 2002/95/EC
- Chinese RoHS SJ/T 11363-2006

MTBF reliability prediction

The COM Express module has a predicted MTBF in hours at 35°C and 55°C ambient temperatures as shown in Table 14. The predictions are based on Telcordia® SR-332 Issue 2, Method 1, Case III with the following underlying assumptions:

- Ground benign in a controlled environment
- 50% default stress ratio for all modeled components
- 100% operating duty cycle
- Level II quality grade on all components
- Mechanical components are not modeled
- No burn-in or pre-testing specified
- Relex Studio® 2009 modeling software
- No component-specific thermal rises or other voltage/current stress applied
- Results rounded to nearest thousand

Table 14. MTBF reliability

Model	Product code	MTBF at 35°C	MTBF at 55°C
C-Temp	CEQM77-3612-0	720,703 hours	304,359 hours
	CEQM77-3615-0	690,050 hours	284, 712 hours
	CEQM77-3610-0	720,703 hours	304,359 hours
	CEQM77-3517-0	741,277 hours	317, 420 hours
	CEQM77-3555-0	741,277 hours	317, 420 hours

Hardware Reference

General specifications

Table 15. CEQM77 general specifications

Feature	Function	Description
Physical	Dimensions	125mm x 95mm
	COM Express	• Basic form factor as defined in the *PICMG COM.0 COM Express Basic Specification Revision 2.0* • COM Express Type 6 pinouts • Board-to-board interconnectors comprising two 220-pin, 0.5mm pitch receptacles
Processor	BGA options	Intel Ivy Bridge product family: • Intel Core i7-3612QE processor, 2.1GHz, quad-core • Intel Core i7-3615QE processor, 2.3GHz, quad-core • Intel Core i7-3517UE processor, 1.7GHz, dual-core • Intel Core i7-3555LE processor, 2.5GHz, dual-core • Intel Core i5-3610ME processor, 2.7GHz, dual-core
Chipset		Intel QM77 platform controller hub (PCH)
Memory	Type	Two 204-pin right-angle SO-DIMM sockets for 1333 MT/s or 1600 MT/s DDR3 SDRAM, without ECC
	Capacity	1GB – 16GB (8GB per channel)
Video		• PCI Express x16 graphics interface • Single channel and dual-channel, 18-bit and 24-bit LVDS • Analog VGA • DDI 1 (PCH Port B) for DisplayPort, HDMI or SDVO support • DDI 2 (PCH Port C) for DisplayPort or HDMI support • DDI 3 (PCH Port D) for DisplayPort or HDMI support • DDI 3 (PCH Port D) for eDP support • Integrated graphics supports three independent displays
Audio		• One High Definition Audio interface • Audio stream output through HDMI or DisplayPort • One Speaker Out interface

Table 15. CEQM77 general specifications (continued)

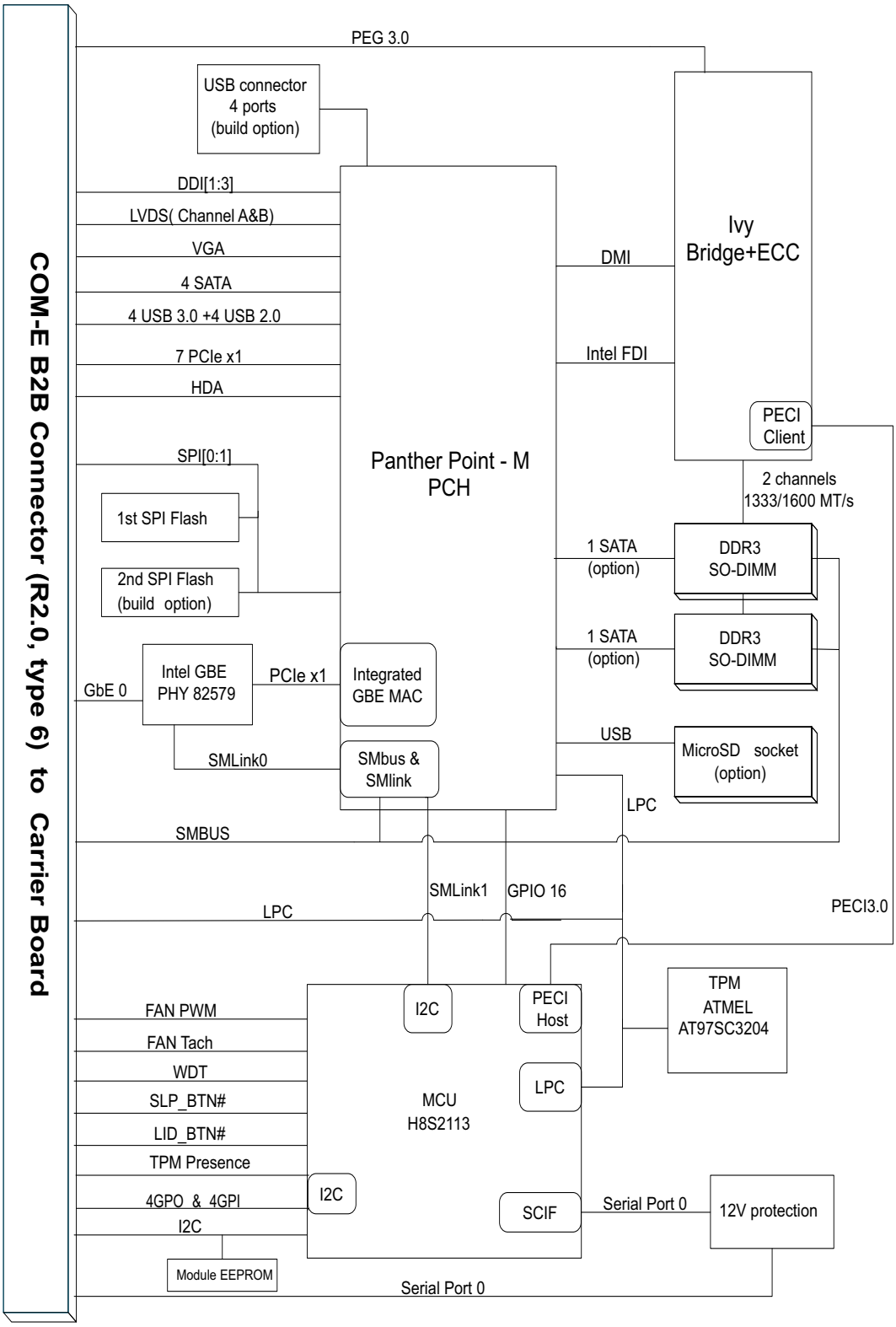
Feature	Function	Description
Storage I/O	SATA	• Four SATA interfaces, ports [0:1] with a PHY data transfer rate of up to 6.0Gbps, ports [2:3] with a PHY data transfer rate of up to 3.0Gbps • Support for SATA hard disk drives, solid state drives, and CD/DVD-ROM drives • Support for AHCI and RAID (RAID 0, RAID 1, RAID 5, and RAID 10) modes • Support for Virtium SSDDR with 8 – 32 GB NAND flash as a build option (for non-ECC modules) • Support for the second BIOS flash as a build option • Support for microSD as a build option
General I/O	GPIO	• Eight GPIO pins (four GPI, four GPO) • GPI3 routing options as ACPRESENT (for AC power detection) and GPI3 (for general-purposed GPIO) on the board-to-board interconnectors (to be configured by BIOS setup utility) • GPI2 multiplexed as ICCMON to monitor the charger current
	I^2C	One I^2C interface
	LPC	One LPC interface
	PCI Express	• One PCI Express x4 interface (lanes [0:3]), configurable as one x4 interface, two x2 interfaces, one x2 interface plus two x1 interfaces, or four x1 Interfaces • Two PCI Express x1 interfaces (lanes [4:5]), configurable as one x2 interface or two x1 interfaces • One PCI Express x1 interface (lane 6) • Support for two ExpressCard modules • PCI Express lane width options configuration via soft straps in the BIOS flash descriptor
	Serial	One 16550-compatible serial port
	SMBus	One SMBus interface
	USB2.0 USB3.0	• Eight USB 2.0 ports [0:7] (the first 4 of 8 ports support USB 3.0) • USB 2.0 Debug Port on port 0 • Support for Self-Power mode application as a build option • Support for USB flash drives, hard disk drives, floppy drives, CD-ROM/DVD-ROM drives, keyboard, mouse, and USB hubs
	Legacy support	• BIOS support for SMSC® LPC47N217/47N207, Nuvoton® WPCN383U, Winbond® W83627DHG-P, and SMSC SCH3116 LPC Super I/O legacy devices • Legacy-free operation via BIOS auto-detection
Network		• Single auto-negotiation 10/100/1000Mbps Base-T Ethernet • IEEE 802.3ab compliant • Programmable Ethernet LEDs for link, activity, and speed

Table 15. CEQM77 general specifications (continued)

Feature	Function	Description
BIOS		• Up to two 16 MB SPI flash ROMs (one soldered on the module, the other on the carrier board as a build option) • AMI® Aptio® BIOS with Radisys extensions • BIOS readiness for legacy and EFI native operating systems
Thermal management		• Temperature monitoring via the processor's DTS thermal sensor and onboard thermal sensor • Processor and module temperature display in BIOS • Hardware-controlled CPU throttling when the processor reaches its catastrophic temperature limit • OSPM-controlled CPU throttling at the 97°C system temperature and shutdown at 100°C • PCH-based memory bandwidth throttling via BIOS configuration • One fan tach input and PWM output signals for fan control
System	Security	• Support for TPM • Password control against unauthorized BIOS configuration
	Management	• Enhanced Intel® SpeedStep Technology • Intel Hyper-Threading Technology • Intel Trusted Execution Technology • Intel Turbo Boost Technology • Intel Virtualization Technology (VT-x) • Intel Virtualization Technology for Directed I/O (VT-d) • Microsoft® Windows® System-Locked Preinstallation (SLP) support via BIOS customization • Watchdog support
Power	Requirement	• +12V (range: 9V–16.8V) input from carrier board with + 5V standby (optional)
	Management	• ACPI 3.0 states S0, S3, S4, S5, G3, and C0, C1, C3, C6, C7 • Support for Intel Active Management Technology (AMT)'s Management Engine (ME) power states M0, M3, M_{off} • Support for ACPI wake up events: power button, RTC alarm, Wake on LAN, and PCI Express power management event signaling
OS support		• Windows 7 (32-bit and 64-bit) • Windows Embedded Standard 7 (64-bit) • Windows Server 2008 R2 64-bit • Ubuntu® Linux 12.04 LTS (32-bit and 64-bit)
Operating temperature		• CEQM77: 0°C to +60°C ambient temperature

Block diagram

Figure 8. CEQM77 block diagram



Power supply

Power options

The COM Express module is capable of operating under two power supply modes:

- 12V only. The ATX power supply is typically forced on.
- 12V plus +5V standby. The ATX power supply is controlled according to the COM Express module‘s SUS_S3# output.

To select a power supply mode, the carrier board typically provides jumper settings. For example, when a COM Express module is used with a CR300 carrier board, a 12V plus +5V standby power supply to the system will be used by default. Refer to your carrier board documentation for instructions on setting up the power supply.

DC power

Power to the COM Express module comes from the carrier board. There is also a common 3V battery supply for the real-time clock (RTC). Table 16 shows the voltage requirements on DC power.

Table 16. COM Express module‘s power supply requirements

Supply	Current/Watts	Rise time	DC range	Maximum ripple
12V	8A/96W	0.1ms to 20ms	9 to16.8V	100mV @ 0-20MHz
5V standby	1A/5W	0.1ms to 20ms	5V±5%	50mV @ 0—20MHz
3V battery	10µA	0.1ms to 20ms	3.0 to 3.3V	—

Smart battery operation

The system BIOS supports smart battery operation via the ACPI 3.0 control method if the smart battery subsystem is present on the carrier board. The smart battery, smart battery manager, smart battery charger, and smart battery selector connect to the PCH‘s SMBus host controller. For information on the SMBus address on the module used to support smart battery, see *I2C and SMBus on page 42*.

Refer to the *Advanced Configuration and Power Interface Specification Revision 4.0* for further information.

Inrush current

The inrush current to the module depends on the rise time of the main power from the carrier board.

Figure 9 on page 29 and Figure 10 on page 30 show the inrush currents to the COM Express module when the power supply is 12V with 5V standby. Figure 11 on page 31 shows the module inrush current when the power supply is 12V only.

Figure 9. 12V with 5V standby power supply: inrush current at 12V

Figure 10. 12V with 5V standby power supply: inrush current at 5V

Figure 11. 12V power supply: inrush current at 12V

CPU

The Intel Ivy Bridge processor is a 64-bit, multi-core, mobile processor built with 22-nanometer process technology. Based on the low-power, high-performance Ivy Bridge micro-architecture, the processor is designed for a two-chip platform (processor, and PCH) as opposed to the traditional three-chip platforms (processor, GMCH, and ICH).

The COM Express module primarily uses the following processor features. For further information, refer to the Intel processor datasheet available on the Intel Web site, www.intel.com.

- Quad/Dual execution cores
- 32KB instruction and 32KB data first-level cache (L1) for each core
- 256KB shared instruction/data second-level cache (L2) for each core
- Up to 8MB shared instruction/data third-level cache (L3) shared among all cores
- Intel Streaming SIMD Extensions 4.1 (SSE4.1) and 4.2 (SSE4.2)
- Dual-channel DDR3 memory with a maximum of one SO-DIMM per channel
- One 16-lane PCI Express Gen 3 port intended for graphics cards
- Direct Media Interface 2nd Generation (DMI2)
- Integrated GPU (graphics processing unit) with a seventh-generation graphics core refresh
- Intel Flexible Display Interface (FDI)
- Communication via Platform Environment Control Interface (PECI) between a PECI client (the processor) and a PECI master (the PCH)
- Intel 64 Architecture
- Intel Hyper-Threading Technology
- Intel Turbo Boost Technology
- Intel Active Management Technology 8.0 (Intel AMT 8.0)
- Enhanced Intel SpeedStep Technology
- Intel Virtualization Technology (Intel VT-x)
- Intel Virtualization Technology for Directed I/O (Intel VT-d)
- Intel Trusted Execution Technology (Intel TXT)
- Intel Advanced Vector Extensions (Intel AVX)
- Advanced Encryption Standard New Instructions (AES-NI)
- PCLMULQDQ Instruction (performs a carry-less multiplication of two 64-bit integers)
- Execute Disable Bit
- Full support of ACPI processor states C0, C1, C1E, C3, C6, C7

Note: The system BIOS allows you to enable or disable the Intel Virtualization Technology (Intel VT-x), Hyper-Threading Technology, SpeedStep Technology, Trusted Execution Technology, and Turbo Boost Technology. See *System Management on page 50* for instructions.

Specifying the number of active processor cores

If your application requires a high-performance system, it is recommended that you keep all of the CPU cores active. Otherwise, you can disable one core to save power.

You can specify the number of active processor cores in the system setup utility's Configuration > CPU Configuration menu. Refer to the *System Setup Utility Specification for details*.

Once the active core(s) is specified, the system will enter C-states accordingly. See *Processor states on page 56* for a description of C-states.

Platform Controller Hub (PCH)

The Intel Panther Point platform controller hub provides extensive I/O support. The COM Express module primarily uses the following PCH features.

- Compliant with the *PCI Express Base Specification, Revision 2.0*, the PCH supports up to eight ports running at up to 5.0 GT/s
- *ACPI Power Management Logic, Revision 4.0* support
- Enhanced DMA controller, interrupt controller, and timer functions
- Integrated SATA host controllers with independent DMA operation for data transfer rates up to 6.0 Gbps on the first two ports and up to 3.0 Gbps on the remaining ports
- Two USB EHCI host controllers with support for up to fourteen USB ports, among which eight ports are used on the COM Express module
- One xHCI Host Controller with support for up to four SuperSpeed USB 3.0 ports
- *System Management Bus (SMBus) Specification, Version 2.0* with additional support for I^2C devices
- Intel High Definition Audio support
- LPC/FWH interface
- Integrated Gigabit Ethernet controller with integrated MAC
- Serial Peripheral Interface (SPI) support
- Intel Matrix Storage Technology
- Intel Virtualization Technology for Directed I/O (Intel VT-d)
- Intel Trusted Execution Technology
- Intel Anti-Theft Technology
- Intel Active Management Technology with System Defense
- JTAG Boundary Scan support
- Integrated TPM 1.2
- 25mm x 25mm FCBGA Package
- Analog and Digital Display Ports (VGA, LVDS, SDVO…)
- Integrated Clock Controller
- Dual Channel NAND Interface supporting 1.8V ONFi 2.0-compliant NAND flash

The system BIOS allows you to enable or disable the Intel Virtualization Technology for Directed I/O (Intel VT-d). See *System Management on page 50* for instructions.

Note: PCI Express cards using non-common clock modes are not supported in this platform.

System memory

DDR3 SDRAM

CEQM77 modules have two 204-pin, right-angle SO-DIMM sockets (S1, S2) to accept DDR3 SDRAMs. At least one SDRAM or SSDDR is required to make the system operational.

For a list of the system memory that Radisys has validated for use with the COM Express module, refer to the *Approved Components List*.

System memory interface features include support for:

- DDR3 SDRAM with transfer rates of 1333 MT/s or 1600 MT/s (see *General specifications on page 24* for details)
- 1GB, 2GB, 4GB, and 8GB DDR3 SDRAM densities
- 64-bit wide channels
- x8 and x16 DDR3 devices
- DDR3 on-die termination (ODT)
- Simultaneous operation of two memory channel configurations:
  - Dual-Channel Symmetric (with Interleaved access)
  - Dual-Channel Asymmetric (with or without Intel Flex Memory Technology)

Video

PCI Express Graphics

The PEG interface originates from the Intel Ivy Bridge processor and connects to PCI Express lanes [16:31] on the board-to-board interconnectors. PCI Express lane 16 is also known as PEG lane 0, and PCI Express lanes [16:31] are known as PEG lanes [0:15] or the PEG slot.

PEG features include:

- Compliance with the *PCI Express Base Specification, Revision 3.0*
- Support for Gen3 (8 GT/s) PCI Express frequency
- Support for Low Swing (low-power/low-voltage) and Full Swing operating modes
- Support for static land numbering reversal

Configuring the PCI Express Graphics (PEG)

To configure graphics on the PCI Express x16 slot:

1. During system startup, press <F2> or <Delete> to enter the system setup utility.
2. In the Configuration > PCI Express Graphics (PEG) Configuration menu, set PCI Express Graphics to [Auto detect] or [Always enabled].
3. To save power, set ASPM Support to [Auto] so that PEG devices will operate with the PCI Express Active State Power Management (ASPM) mode. This may slightly affect PEG performance.
4. In the Save & Exit menu, choose Save Changes and Restart.

Configuring PEG lane usage

The PEG interface can support one x16, two x8, and one x8 plus two x4 ports via PCI Express lane soft strap configuration. Each x8 interface supports x1, x2, x4, and x8 devices. Lane usage is displayed in the system setup utility's Configuration > PCI Express Graphics (PEG) Configuration menu.

- If the carrier board serial EEPROM is detected, the embedded controller will automatically configure the strap pins via the PEG lane descriptor information that resides in the carrier board EEPROM.
- If no relevant EEPROM content is detected, you can configure the PEG lane usage with the PCI Express Soft Strap Edit tool "Rsyspcie" utility. For configuration instructions, refer to the readme file that comes with the utility.

VGA

The COM Express module supports an analog CRT interface via the Intel Graphics Media Accelerator 7.0 controller.

VGA interface features include:

- DAC frequencies up to 340.4 MHz
- Render frequencies are dynamically selected by the graphics driver according to the graphics workload, as permitted by Intel Turbo Boost Technology
- 24-bit RAMDAC
- Support for analog monitor resolutions up to QXGA (2048x1536 @75 Hz)

LVDS

The COM Express module supports an LVDS interface via the integrated Intel Graphics Media Accelerator 7.0 controller. LVDS interface features include:

- Automatic display resolution. The Intel video BIOS will automatically configure the integrated LVDS display to use one of the resolutions below. If the BIOS cannot detect the LVDS flat panel's optimal resolution, the default resolution of 1024x768 will be used.
  - 800x600
  - 1024x768
  - 1280x768
  - 1280x800
  - 1280x1024
  - 1400x1050
  - 1600x1200
  - 1680x1050
  - 1920x1200
- 25–112MHz single-channel and dual-channel LVDS interfaces
  - The single-channel LVDS interface supports one 18-bpp or one 24-bpp panel (Type 1 only, compatible with VESA LVDS color mapping)
  - The dual-channel LVDS interface supports two 18-bpp or two 24-bpp panels

  Note: In single-channel mode, Channel B of the two LVDS transmitter channels cannot be used.
- Pixel dithering for 18-bit TFT panel to emulate 24-bpp true color displays
- Panel fitting, panning, and center modes
- Spread spectrum clocking
- Integrated PWM interface for LCD backlight inverter control
- Compatible with the ANSI/TIA/EIA-644 specification

You can configure the LVDS resolution and backlight brightness for use prior to entering the operating system. These settings are specified in the system setup utility's Configuration > Integrated Video Configuration menu. Refer to the *System Setup Utility Specification* for details.

Digital display interfaces

The COM Express module's PCH chipset integrates three digital display ports (B, C, and D). Each port supports one of the following interfaces on the carrier board:

- Port B (DDI 1) supports DisplayPort, HDMI, or SDVO
- Port C (DDI 2) supports DisplayPort or HDMI
- Port D (DDI 3) supports DisplayPort, HDMI, or embedded Display Port

Each DDI port is capable of driving a digital display up to 2560x1600 @ 60 Hz using DisplayPort and 1920x 1200 @ 60 Hz using HDMI or DVI (with reduced blanking).

DisplayPort

DisplayPort is a digital communication interface that utilizes differential signalling to achieve a high bandwidth bus interface for connections between computers and displays (monitors, projectors, and TVs). DisplayPort is also suitable for display connections between consumer electronics devices, such as high definition optical disc players, set top boxes, and TVs.

When DisplayPort interfaces are in use, the system BIOS will automatically detect and configure the installed devices according to settings in the video BIOS.

Embedded DisplayPort

The processor has an embedded DisplayPort (eDP) interface that is disabled by default. When enabled, the dedicated eDP interface is not physically shared with the PEG interface; it is routed to the PCH chipset's Port 3 (DDI 3).

Embedded DisplayPort features include:

- 1.62 Gbps and 2.7 Gbps link speeds on 1, 2, or 4 data lanes
- Support for –0.5% SSC and non-SSC clock settings

HDMI

A High-Definition Multimedia Interface (HDMI) is provided for transmitting uncompressed digital audio and video signals from AV sources such as DVD players and set-top boxes to television sets, projectors, and other video displays. The HDMI interface can carry high-quality, multi-channel audio data, as well as all standard- and high-definition consumer electronics video formats.

The HDMI interface originates from the PCH and utilizes transition minimized differential signaling (TMDS) to carry audiovisual information through the HDMI cable. Audio, video and auxiliary (control/status) data are transmitted across the three TMDS data channels.

When DisplayPort interfaces are in use, the system BIOS will automatically detect and configure the installed devices according to settings in the video BIOS.

SDVO

The SDVO port is configured through the PCH Digital Port B, and is capable of driving at a pixel rate of 200 MP/s.

SDVO features include:

- Downstream HDCP support (no upstream HDCP support)
- Display hot plug support
- I^2C channel provided for control
- Support for external SDVO components (CRT/LVDS/TV/DVI)
- Support for Radisys media expansion cards (Radisys product code: MEC-DUAL-LVDS). For further information, refer to the *Media Expansion Cards Product Manual*.

Configuring the primary display

By default, when the system BIOS detects the presence of a PCI Express and/or a PCI graphics card in the system, the PCI Express graphics display will be given first priority, then the PCI graphics display, and finally any integrated displays.

To select a specific primary display:

1. During system startup, press <F2> or <Delete> to enter the system setup utility.
2. In the Configuration > Integrated Video Configuration menu, set Primary Display to the desired option:
   - Auto (default)
   - IGD (See *Specifying the graphics source for your LFP on page 39* for instructions on choosing the graphics source for your local flat panel, which can be either LVDS or embedded DisplayPort.)
   - PEG
3. In the Save & Exit menu, choose Save Changes and Restart.

Configuring the boot display

Only the integrated video can be recognized and used during system startup. By default, the system BIOS will automatically detect the attached video device for the boot display according to the video BIOS algorithm.

To select a specific boot display:

1. During system startup, press <F2> or <Delete> to enter the system setup utility.
2. In the Configuration > Integrated Video Configuration menu, set Primary Boot Display to the desired option:
   - Auto (default)
   - CRT

- LFP — The integrated LVDS will be used by default. See *Specifying the graphics source for your LFP on page 39* for instructions on choosing the SDVO LVDS or embedded DisplayPort graphics source for your LCD flat panel.

In the Configuration > Integrated Video Configuration menu, there is also an option to set up a second boot display:

- Disabled (default)
- CRT
- LFP

Note: This option is not available when the Primary Boot Display is set to [Auto].

3. Set the LVDS Panel Resolution to the desired value.
4. In the Save & Exit menu, choose Save Changes and Restart.

Specifying the graphics source for your LFP

When the COM Express module is configured to use the integrated graphics, the system BIOS allows you to configure the graphics source for the local flat panel (LFP) attached to your carrier board. An LFP can be either an LVDS flat panel or an embedded DisplayPort device.

To specify the graphics source for your LFP:

1. During system startup, press <F2> or <Delete> to enter the system setup utility.
2. Navigate to the Configuration > Integrated Video Configuration menu.
3. Optional. To set up the LFP for use under the operating system, set Primary Display to [IGD]. To set up the LFP for use prior to entering the operating system, set Primary Boot Display to [LFP].
4. Set Active Local Flat Panel to the desired option:
   - None — The system will not output video to any LFP
   - Integrated LVDS (default)
   - SDVO LVDS
   - eDP
5. In the Save & Exit menu, choose Save Changes and Restart.

Configuring the video memory

The system BIOS uses the Dynamic Video Memory Technology (DVMT) to dynamically allocate system memory for use as video memory, which ensures the most efficient use of available resources for maximum 2D/3D graphics performance. If a graphics-intensive application such as a game or a DVD movie requires more memory than the amount of pre-allocated video memory, DVMT will send a request to the operating system for additional, temporary memory.

Pre-allocated memory is the small amount of system memory made available for video by the system BIOS during boot-up. By default, 64MB is used, but you can change the pre-allocated memory to 32MB or 128MB in the system setup utility. The specified pre-allocated amount of memory will not be available for use by the operating system.

The maximum amount of memory that DVMT can request from the operating system can be 128MB, 256MB, or the maximum available system memory depending on your real application needs.

It is recommended that you determine a good balance between BIOS- and operating system-required memory resources. Typically, use less pre-allocated video memory and total DVMT memory for legacy video devices and more video memory when graphics-intensive applications will be used.

To configure the video memory:

1. During system startup, press <F2> or <Delete> to enter the system setup utility.
2. In the Configuration > Integrated Video Configuration menu, adjust the DVMT Pre-allocated Memory and DVMT Total Graphics Memory settings as required.
3. In the Save & Exit menu, choose Save Changes and Restart.

Video display options

The COM Express module supports three or more independent displays using any of the three integrated display ports. Additional display port(s) can be added using an external GPU add-in card installed in a PCI Express port.

Multi-monitor display modes include:

- Single pipe, single display: one port is activated to display the output on one device.
- Intel dual display clone: both display ports are activated to display the same output to two different display devices. The displays must have the same color depth setting, but can use different refresh rates and resolution settings.
- Extended desktop: both display ports are activated to display two different outputs to two different display devices. The devices have different color depths, refresh rates, and resolution settings.

Audio

The PCH's High Definition Audio (HDA) controller provides a digital interface that can attach up to four CODECs of different types, such as audio and modem CODECs.

The COM Express module can also generate a PC speaker signal for diagnostic beeps. The carrier board may support an onboard PC speaker or PC speaker pinouts on the front I/O panel.

Configuring the HDA

To enable HDA:

1. During system startup, press <F2> or <Delete> to enter the system setup utility.
2. In the Configuration > Advanced Configuration menu, set HDA to [Enabled] or [Auto].
3. In the Save & Exit menu, choose Save Changes and Restart.

Storage I/O

SATA

Four SATA 2.0 ports support independent DMI operation via the two integrated SATA host controllers on the PCH chipset.

SATA interface features include:

- Support for data transfer rate up to 6.0Gbps
- Support for SATA hard disk drives, solid state drives (SSD), and CD-ROM/DVD-ROM drives
- IDE, AHCI, and RAID (0, 1, 5, and 10) modes

By default, the system BIOS supports SATA operation. Each SATA port can be enabled or disabled individually in the system setup utility's Configuration > SATA Configuration menu. The system BIOS will detect the presence of SATA devices. When present, the devices will be displayed in the system setup utility.

Note: Each SATA port can be enabled or disabled individually only when SATA Mode is set to [AHCI] or [RAID] in the system setup utility's Configuration > SATA Configuration menu.

To disable SATA operation:

1. During system startup, press <F2> or <Delete> to enter the system setup utility.
2. In the Configuration > SATA Configuration menu, set SATA Operation to [Disabled].
3. In the Save & Exit menu, choose Save Changes and Restart.

General I/O

General Purpose I/O (GPIO)

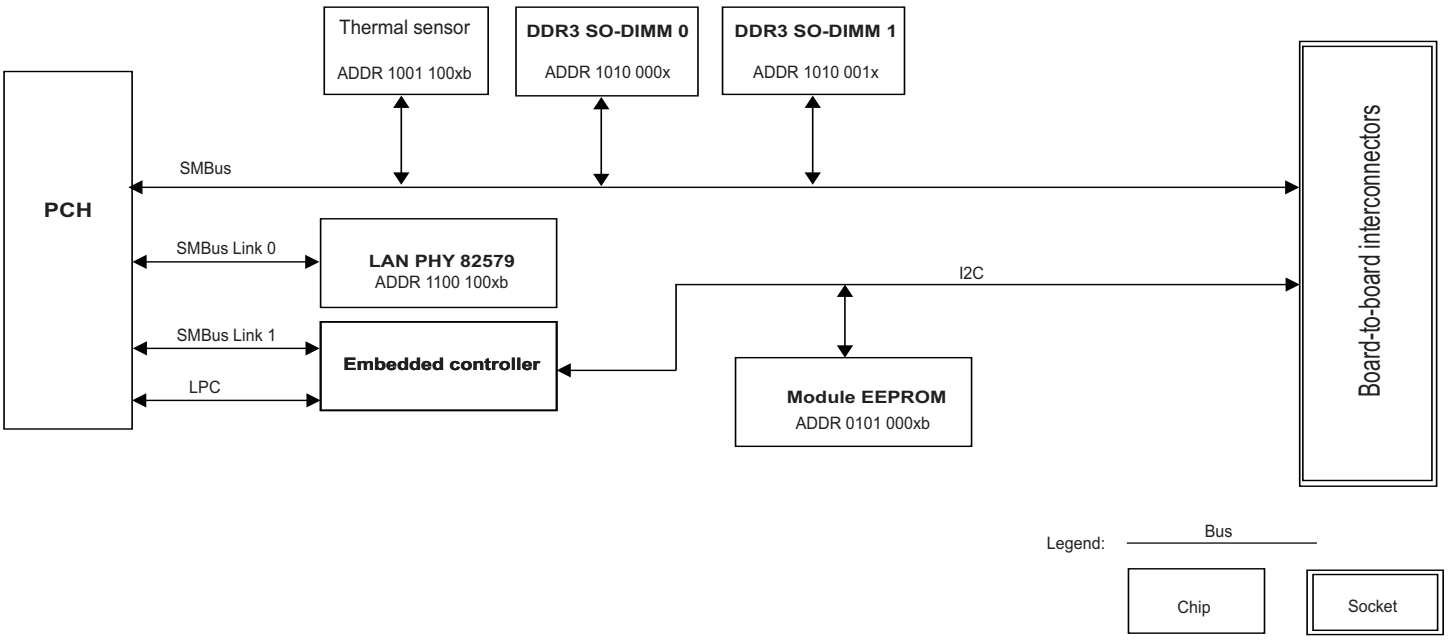
The COM Express module supports four GPIs [0:3] and four GPOs [0:3] through the PCH chipset and the embedded controller.

In the system setup utility, you can determine whether GPI3 is routed to the PCH's ACPRESENT signal or to the PCH's general-purpose GPIO16. Assertion of the ACPRESENT signal is required to support Intel Turbo Boost Technology. See *Intel Turbo Boost Technology on page 51* for instructions.

I²C and SMBus

The COM Express module provides both SMBus and I²C buses to the carrier board. The SMBus is connected to the PCH, and the I²C bus is connected to the EC. Figure 12 shows the I/O addresses used by the SMBus and I²C bus device routing.

Figure 12. I²C and SMBus device routing



Low Pin Count (LPC)

The COM Express module provides an LPC interface, which complies with the *LPC 1.1 Specification* and supports two master/DMA devices. This interface allows the connection of devices such as Super I/O, micro controllers, and customer ASICs.

The Port80 Power On Self Test (POST) codes are output to the LPC bus. For further information, see *BIOS Configuration and OS Support on page 64*.

PCI Express

The COM Express module supports seven PCI Express expansion ports (lanes [0:6]) that are compliant with the *PCI Express Base Specification Version 2.0*. Each port supports 5GBps bandwidth in each direction.

The system BIOS can use the PCI Express power management event signal (PME) to wake up the system from the S3, S4, and S5 power states. PME wake-up is enabled by default.

ExpressCard support

Two PCI Express-based ExpressCard modules are supported via the EXCD[0:1]_PERST# and EXCD[0:1]_CPPE# signals.

Each ExpressCard interface requires one PCI Express lane. The carrier board design will determine which PCI Express lanes are used for ExpressCard modules.

Configuring link options for PCI Express expansion ports

The COM Express module allows PCI Express lanes [0:6] link options to be set up by soft straps in the BIOS flash descriptor.

- Lanes [0:3] can be statically configured as one x4 interface, two x2 interfaces, four x1 interfaces, or one x2 interface (lanes [0:1]) and two x1 interfaces (lanes [2:3]).
- Lanes [4:5] can be configured as one x2 interface or two x1 interfaces.
- Lane 6 always functions as one x1 interface.

If you use the PCI Express Soft Strap Edit tool “Rsyspcie” to configure PCI Express lane width options, ensure that the following conditions are met:

- Some of the lanes [0:7] may be routed to system interfaces or devices on the COM Express module and cannot be used for general-purpose I/O support. When selecting a lane width option for lanes [0:3] or lanes [4:7], the selected lanes must remain in x1 operational mode or there may be a loss in functionality. For example, on the CEQM77 modules, lane 7 connects to the Gigabit Ethernet controller.
- PCI Express lanes specifically allocated for ExpressCard modules must remain in x1 operational mode or ExpressCard modules will not work.

Serial port

The embedded controller supports one 16550-compatible serial port and the signals are routed to the board-to-board interconnectors.

To configure this serial port:

1. During system startup, press <F2> or <Delete> to enter the system setup utility.
2. In the Configuration > Advanced Configuration menu, set Serial Port on Module to [Enabled] or [Disabled].
3. If you need to set up console redirection on this serial port, see *Console redirection on page 65* for instructions.
4. In the Save & Exit menu, choose Save Changes and Restart.

Note: The COM Express module may support another one, two, or six legacy serial ports if the carrier board contains a suitable LPC Super I/O chip. See *Legacy support on page 46* for information on LPC Super I/O chip support. Refer to the *System Setup Utility Specification* for further information.

SPI flash

The PCH chipset has two SPI chip-select signals, SPI_CS[0:1]#, to support SPI-compatible flash devices with up to 16MB flash ROM. The SPI source may come from the PCH's SPI0 or SPI1.

- Up to two onboard 8MB SPI flash chips can be built onto the CEQM77 modules. One is soldered onto the module and contains the BIOS firmware code. The second SPI flash is available as a build option.
- When the carrier board contains an SPI flash chip, it is possible to boot the system from the BIOS ROM on the carrier board.

Two boot BIOS selection straps, BIOS_DIS[0:1]#, are used to determine whether to boot the system from the SPI BIOS on the module or from the SPI BIOS on the carrier board. The carrier board typically provides jumper selections (or equivalent) to choose the BIOS boot device.

Table 17 shows the effect of the BIOS_DIS[0:1]# signals when the appropriate configuration is set on the carrier board.

Table 17. Effect of the BIOS disable signals

BIOS_DIS1#	BIOS_DIS0#	Carrier SPI_CS#	SPI Descriptor	Boot BIOS From...
0	0	SPI1	Module	Module SPI ROM
0	1	SPI0	Carrier	Carrier SPI ROM
1	1	High[1]	Module	Module SPI ROM

[1] High means SPI ROM on the carrier board is not selected.

Supplying power to the carrier SPI

The COM Express module provides an SPI_POWER pin on the board-to-board interconnectors to supply nominally 3.3V suspend/3.3V, 100mA power to the SPI bus on the carrier board. The carrier board must use less than 100mA of SPI_POWER.

Note: SPI_POWER must only be used to power SPI devices on the carrier board. The carrier board must use SPI_POWER from the COM Express module to supply the power to the carrier board's SPI bus, otherwise incompatibilities or power rail leakage may occur.

USB

The Panther Point PCH contains up to two Enhanced Host Controller Interface (EHCI) host controllers that support USB high-speed signaling on up to fourteen USB 2.0 ports. High-speed USB 2.0 allows data transfers up to 480 Mbps.

The PCH also contains an eXtensible Host Controller Interface (xHCI) host controller that supports up to four USB 3.0 ports. This controller allows data transfers up to 5 Gbps, which is 10 times faster than high-speed USB 2.0.

PCH USB ports 1, 0, 2, 3, 8, 9, 10, and 11 are routed through the board-to-board connector USB [0:7]. PCH USB port 1 is a USB debug port that is routed (board-to-board) to USB Port 0.

USB features support:

- Super-speed, high-speed, full-speed, and low-speed USB
- USB3.0 SuperSpeed on four of eight USB2.0 expansion ports
- USB hard disk drives, flash drives, floppy disk drives, and CD-ROM/DVD-ROM drives
- High-speed USB 2.0 debug port on USB port 0
- Console redirection on USB port 0 with a debug cable

Configuring USB port(s)

In the system BIOS, you can configure specific USB ports individually. By default, all ports are enabled.

To configure the USB port(s):

1. During system startup, press <F2> or <Delete> to enter the system setup utility.
2. In the Configuration > USB Configuration menu, set the desired ports to [Enabled] or [Disabled].
3. In the Save & Exit menu, choose Save Changes and Restart.

To configure the USB 3.0 support:

1. During system startup, press <F2> or <Delete> to enter the system setup utility.
2. In the Configuration > USB Configuration menu, set USB 3.0 Support to [Enabled] or [Disabled].

In the Save & Exit menu, choose Save Changes and Restart.

Configuring the USB debug port

USB port 0 can be used as the USB 2.0 debug port. A USB 2.0 debug cable is required. Follow the steps in the preceding section, and make sure that USB Port 0 is enabled in the system BIOS.

Legacy support

The system BIOS can support RS-232 serial ports and PS/2 keyboard and mouse when the carrier board contains any of these LPC Super I/O chips:

- SMSC® LPC47N217/47N207
- Nuvoton® WPCN383U
- Winbond® W83627DHG-P
- SMSC SCH3116

RS-232 serial ports support console redirection to extend video display during system startup. See *Console redirection on page 65* for instructions.

Tip: The COM Express module also supports a 16550-compatible serial port on the board-to-board interconnectors. See *Serial port on page 44* for details.

Ethernet

The COM Express module supports one 10/100/1000 Mbps Ethernet interface via the Intel 82579 Gigabit Ethernet controller.

Ethernet features include:

- Gigabit Ethernet support via the PCI Express x1 interface
- 10/100/1000 Mbps full-duplex and half-duplex operation
- IEEE 802.3x-compliant flow control support with software controllable pause times and threshold values
- IEEE802.3ab auto-negotiation support and IEEE802.3ab PHY compatibility
- Full wake-up support
- Four programmable LEDs for link status, traffic, 100Mbps speed, and 1000Mbps speed

Configuring Wake On LAN

The Ethernet connection must be active for Wake On LAN. To wake up the system from the S3, S4, and S5 power states:

1. During system startup, press <F2> or <Delete> to enter the system setup utility.
2. In the Configuration > LAN Configuration menu, set Onboard LAN and Wake On LAN to [Enabled].
3. In the Save & Exit menu, choose Save Changes and Restart.

Note: The Intel Management Engine (ME) M3 power state must be enabled during the system startup before the Wake On LAN item can be configured in the system setup utility.

Configuring PXE boot

To boot from the network:

1. During system startup, press <F2> or <Delete> to enter the system setup utility.
2. In the Configuration > LAN Configuration menu, make sure Onboard LAN is set to [Enabled].
3. Set Wake On LAN and PXE Option ROM to [Enabled].
4. In the Boot menu, set Boot Option #1 to the Ethernet device. If you have omitted Step 3, the network boot agent will be unavailable in the Boot Option Priorities list.
5. In the Save & Exit menu, choose Save Changes and Restart.

Tip: If you do not need to boot from the network each time, you can set the network device to a lower priority in the Boot menu. When the system restarts, press <F7> to enter the Boot Action menu, and select the network device to continue PXE boot.

Real-time clock (RTC)

The PCH contains a Motorola® MS146818B-compatible real-time clock with 256 bytes of battery-backed RAM. The real-time clock performs two key functions: keeping track of the time of day and storing system data, even when the system is powered down. The RTC operates on a 32.768 KHz crystal and a 3V battery.

Note: Once the RTM battery is removed from the carrier board, the last BIOS settings are still present in the SPI flash ROM. However, the system date and time may revert to their default settings.

Setting the RTC alarm time

The system supports a 24-hour RTC alarm to wake the system from the S3, S4, and S5 power states. By default, the RTC alarm is disabled.

To wake the system at a specified time:

1. During system startup, press <F2> or <Delete> to enter the system setup utility.
2. In the Configuration > Power Control Configuration menu, set RTC Alarm to [Enabled], and select a specific time from the options presented or enter numerical values from the keyboard:
   - Wake-up Hour: 0 – 23
   - Wake-up Minute: 0 – 59
   - Wake-up Second: 0 – 59
3. In the Save & Exit menu, choose Save Changes and Restart.

Setting an alarm interval

As an alternative to setting a specific wake up time, you can set a time interval for the system to wake after it enters sleep mode. By default, the RTC alarm is disabled.

To set the time interval:

1. During system startup, press <F2> or <Delete> to enter the system setup utility.
2. In the Configuration > Power Control Configuration menu, set RTC Alarm Interval to [Enabled].
3. Set the Wake-up Interval (minutes) to the desired option, or type a number (1–5) from the keyboard.
4. In the Save & Exit menu, choose Save Changes and Restart.

Security

Trusted Platform Module (product option)

The CEQM77 supports one ATMEL® AT97SC3204 single-chip TPM 1.2 module through the LPC interface. The ATMEL AT97SC3204TPM is unavailable to indicate the physical presence of an operator for certain TPM operations.

By default, TPM is enabled and the current TPM module information will be displayed in the system BIOS. Note that TPM is not supported under the S3, S4, and S5 power states.

To disable TPM functionality:

1. During system startup, press <F2> or <Delete> to enter the system setup utility.
2. In the Configuration > TPM/TXT Configuration menu, set TPM to [Disabled].
3. In the Save & Exit menu, choose Save Changes and Restart.

Password control

Without in-depth knowledge of the system, changes to the advanced BIOS settings may cause serious hardware problems and fatal system errors. The system BIOS allows you to specify an Administrator password with full control and a User password with limited access to the BIOS settings.

To set the password:

1. During system startup, press <F2> or <Delete> to enter the system setup utility.
2. In the Security menu, set an Administrator password and then a User password. It is recommended that you set both passwords. If only the User password is set, the password will be required when the user powers on the system and enters the system setup utility. Once in the system setup utility, the user will then have full control over the BIOS as an Administrator.
3. In the Save & Exit menu, choose Save Changes and Restart.

System Management

Intel Hyper-Threading Technology

With a Hyper-Threading Technology (HT Technology) enabled chipset, BIOS, and operating system, each core in a single physical processor package functions as multiple logical processors.

By default, HT Technology is enabled. To disable support for this technology:

1. During system startup, press <F2> or <Delete> to enter the system setup utility.
2. In the Configuration > CPU Configuration menu, set Intel Hyper-Threading to [Disabled].
3. In the Save & Exit menu, choose Save Changes and Restart.

Enhanced Intel SpeedStep Technology (EIST)

The processor uses the Enhanced Intel SpeedStep Technology (EIST) to centralize the control mechanism in the processor. Based on application demands, the processor will dynamically increase or decrease its clock speed and voltage in order to optimize power consumption.

By default, Intel SpeedStep is enabled. To disable support for this technology:

1. During system startup, press <F2> or <Delete> to enter the system setup utility.
2. In the Configuration > CPU Configuration menu, set Intel SpeedStep to [Disabled].
3. In the Save & Exit menu, choose Save Changes and Restart.

Intel Virtualization Technology (Intel VT-x)

The Intel Virtualization Technology (also known as Intel VT) allows a platform to run multiple operating systems and applications in independent partitions. Intel VT-x adds hardware support in the processor to improve the virtualization performance and robustness. Functionality, performance, and other benefits will vary depending on hardware and software configurations.

By default, Intel VT-x is enabled. To disable support for this technology:

1. During system startup, press <F2> or <Delete> to enter the system setup utility.
2. In the Configuration > CPU Configuration menu, set Intel VT-x to [Disabled].
3. In the Save & Exit menu, choose Save Changes and Restart.

Intel Virtualization Technology for Directed I/O (Intel VT-d)

The Intel Virtualization for Direct I/O technology (also known as Intel VT-d) uses the chipset to support and improve I/O virtualization performance and robustness. This technology ensures greater reliability, security, and availability of I/O resources by way of domain-based isolation and virtualization in the GMCH chipset.

Intel VT-d works in conjunction with Intel VT-x described above. Both technologies must be enabled for the system to allow multiple, independent operating systems to run simultaneously.

By default, Intel VT-d is enabled. To disable Intel VT-d:

1. During system startup, press <F2> or <Delete> to enter the system setup utility.
2. In the Configuration > CPU Configuration menu, set Intel VT-d to [Disabled].
3. In the Save & Exit menu, choose Save Changes and Restart.

Intel Trusted Execution Technology (TXT)

The Intel Trusted Execution Technology helps to authenticate the controlling environment so that you can rely on the platform to make an appropriate trust decision. The Intel TXT platform determines the identity of the controlling environment by accurately measuring and verifying the controlling software.

Hardware protection mechanisms will provide trust in the application's execution environment. In turn, this can help to protect vital data and processes from being compromised by malicious software running on the platform.

By default, Intel TXT is enabled. To disable this technology:

1. During system startup, press <F2> or <Delete> to enter the system setup utility.
2. In the Configuration > TPM/TXT Configuration menu, set Intel TXT to [Disabled].
3. In the Save & Exit menu, choose Save Changes and Restart.

Intel Turbo Boost Technology

Intel Turbo Boost Technology is activated when the operating system requests the highest processor performance state (P0). This technology permits processor cores to run faster than the base operating frequency when operating below power, current, and temperature specification limits. By default, Intel Turbo Boost Technology is enabled in the system BIOS to maximize performance.

To configure the Intel Turbo Boost Technology:

1. During system startup, press <F2> or <Delete> to enter the system setup utility.
2. To enable this technology, set Intel Turbo Boost to [Enabled] in the Configuration > CPU Configuration menu.
3. To disable this technology, set Intel Turbo Boost to [Disabled].
4. In the Save & Exit menu, choose Save Changes and Restart.

Note: The maximum operating frequency depends on the number of active cores. See *Specifying the number of active processor cores on page 33* for instructions.

Intel Active Management Technology

Intel Active Management Technology (AMT) is a hardware-based technology for remotely managing and securing computers out-of-band. This technology makes it easier and less expensive for businesses to monitor, maintain, update, upgrade, and repair their computers. Intel AMT is part of the Intel Management Engine (ME), which is built into computers with Intel vPro technology. By default, the Active Management Technology is disabled in the system BIOS.

To configure the Intel Active Management Technology:

1. During system startup, press <F2> or <Delete> to enter the system setup utility.
2. To enable this technology, set Intel AMT to [Enabled] in the Configuration > CPU Configuration submenu. To disable this technology, set Intel AMT to [Disabled].
3. In the Save & Exit menu, choose Save Changes and Restart.

Intel Configurable TDP Technology

Intel Configurable TDP Technology allows users to reconfigure thermal design power (TDP) levels based on the system's current power consumption and heat dissipation capacity.

To configure the TDP levels:

1. During system startup, press <F2> or <Delete> to enter the system setup utility.
2. In the Configuration > CPU Configuration submenu, set Configurable TDP to the desired option:
   - Nominal (default)
   - Up
   - Down
   - Disabled
3. In the Save & Exit menu, choose Save Changes and Restart.

SLP control

An SLP editing tool, "Rsysslp," allows you to customize the SLP Public Key and Windows Marker bin files in the BIOS image. These are used to validate Microsoft Windows System-Locked Preinstallation (SLP) 2.0 and 2.1 for OEM products. The SLP anti-piracy technology helps to prevent the unauthorized copying of Microsoft Windows onto unlicensed computers.

Please contact Radisys to request a copy of this tool if you need it.

Thermal management

The processor contains a digital thermal sensor for each execution core and a thermal monitor to measure the processor temperature. A thermal sensor, Texas Instruments® TMP75, is used to measure the module's temperature. The sensor is an 11-bit digital temperature sensor with a 2-wire SMBus serial interface. For the SMBus address of this thermal sensor, see *I2C and SMBus on page 42*.

The integrated graphics and memory controller (GMC) includes an internal digital thermal sensor for monitoring its temperature and triggering thermal management. The system will dynamically perform bandwidth throttling in response to memory loading or high GMC temperatures. The sensor also supports THERMTRIP# and Render Thermal Throttling.

The two thermal sensors on the PCH monitor the PCH's temperature. The PCH will shut down the system when its thermal limit is reached.

Fan speed

The COM Express module has one fan tach input signal and one PWM output signal. This allows the system BIOS to automatically adjust the fan speed according to the processor temperature that is read by the on-die digital thermal sensor (DTS). The processor and module temperatures are both displayed in the system setup utility's Information > Temperatures and Fan Speed menu. The module temperature is read by the onboard TMP75 thermal sensor.

The system BIOS allows users to set the fan speed for active trip points.

To configure the fan speed:

1. During system startup, press <F2> or <Delete> to enter the system setup utility.
2. In the Configuration > Thermal Control Configuration menu, set Active Trip Point 0 Fan Speed and Active Trip Point 1 Fan Speed to the desired values.
3. In the Save & Exit menu, choose Save Changes and Restart.

Thermal monitoring

The processor and board temperatures are displayed in the system setup utility. To check these temperatures:

1. During system startup, press <F2> or <Delete> to enter the system setup utility.
2. The processor and board temperatures are displayed in the Information > Temperatures and Fan Speed menu.
3. In the Save & Exit menu, choose Save Changes and Restart.

Thermal throttling

Hardware-controlled CPU throttling

The processor must remain within the minimum and maximum junction temperature (Tj) specifications at the corresponding Thermal Design Power (TDP) value. For information about Tj and TDP, see *Thermal specifications on page 20*.

The integrated thermal monitor on the processor can determine when the maximum processor temperature has been reached. If the processor's catastrophic temperature limit of 125°C is detected, the THERMATRIP# signal will be asserted and the voltage supply to the processor turned off within 500ms to prevent permanent silicon damage.

OSPM-controlled thermal management

The system BIOS allows you to configure the active and passive trip points.

To configure the active and passive trip points:

1. During system startup, press <F2> or <Delete> to enter the system setup utility.
2. In the Configuration > Thermal Configuration menu, set Critical Trip Point or Passive Trip Point to the desired values.

   When the Critical Trip Point (default: 100°C) is reached, the operating system-directed power management (OSPM) shuts down the system; when the Passive Trip Point (default: 95°C) is reached, the OSPM starts processor throttling.
3. In the Save & Exit menu, choose Save Changes and Restart.

Memory throttling

When there is a thermal sensor on the DIMM, the COM Express module can use Closed Loop Thermal Throttling (CLTT) for memory bandwidth throttling. The embedded controller will alert the memory controller via PECI when the system memory exceeds its normal operating temperature.

To configure memory bandwidth throttling based on temperature readings from the DIMM's thermal sensor:

1. During system startup, press <F2> or <Delete> to enter the system setup utility.
2. In the Configuration > Thermal Control Configuration menu, set Thermal Sensor on DIMM to [Enabled] or [Disabled]. By default, this item is disabled.
3. In the Save & Exit menu, choose Save Changes and Restart.

Power management

The COM Express module supports the Advanced Configuration and Power Interface (ACPI) 3.0 standard for user-managed power via the operating system. The extent of ACPI support depends on the attached carrier board.

System states

Table 18 shows the supported ACPI states for carrier board power options.

Indicates normal module states.

* Indicates the states entered by software control via ACPI interfaces.

Table 18. Supported ACPI states for 12V power options

VCC state		Description	Supported module states				
5V_SBY	12V		G0/S0[1]	G1/S3[2]	G1/S4[3]	G2/S5[4]	G3[5]
Off	Off	Power off	—	—	–	—	Yes
Off	On	Carrier board with no standby support	Yes	Yes*	Yes*	Yes*	—
On	Off	Standby	—	Yes	Yes	Yes*	—
On	On	Full power	Yes	Yes*	Yes*	Yes*	—

1 G0/S0: Fully operational; working.

2 G1/S3: Standby (suspend to RAM). Main memory is still powered. This state allows the resumption of work exactly where it was left at the start of standby.

3 G1/S4 — Standby (suspend to disk). All content of main memory is saved to non-volatile memory such as a hard disk drive, and is powered down.

4 G2/S5: Soft off. All devices are unpowered. Memory content and context are lost.

5 G3: Mechanical off. System is unpowered with no standby rails. No wake-up is possible.

ACPI wake-up

When 12V operating power and 5V standby power is available from the power supply, the COM Express module is capable of supporting these wake-up events from S3, S4, and S5 power states:

- Power button
- RTC alarm. See *Real-time clock (RTC) on page 48* for instructions.
- Wake On LAN. See *Configuring Wake On LAN on page 47* for instructions.
- PCI and PCI Express power management event signaling. PME wake-up is enabled by default.

Processor states

The C processor power states specify processor power consumption and thermal management within the global working state, G0. The normal CPU operating mode is C0, which is fully powered on. The higher the C number, the deeper the CPU sleep mode. As more circuits and signals are turned off, more time is required for the CPU to wake up.

In general, deeper C-states such as C6 or C7 have long latencies and higher energy entry/exit costs. The resulting performance and energy penalties become significant if the deeper C-states are entered and exited frequently. Over-using the deeper C-states will also shorten the life of the battery. To improve battery life in the deeper C-states, the processor supports two C-state auto-demotion options:

- C6/C7 to C3
- C6/C7/C3 To C1

Table 19 describes the C-states at the core level, and Table 20 on page 57 summarizes how the processor enters the C-state at the package level.

Table 19. Core C-states

Core C-state	Function
C0	The CPU is fully powered and operational.
C1	Stops the main internal CPU clocks via software HLT function or the MWAIT instruction. The bus interface unit and advanced programmable interrupt controller (APIC) are kept running at full speed. The CPU can respond to important requests coming from the external bus and can handle interruptions.
C1E	Stops the main internal CPU clocks via software HLT function or the MWAIT instruction and reduces CPU voltage. The bus interface unit and APIC are kept running at full speed. The CPU can respond to important requests coming from the external bus and can handle interruptions, but the CPU power consumption is lower than C1.
C3	Stops all internal CPU clocks by initiating a P_LVL2 I/O read to the P_BLK or an MWAIT(C3) instruction. The CPU can no longer respond to interruptions or important requests coming from the external bus.
C6	Reduces the CPU core voltage to any value including 0V.
C7	The core C7 state exhibits the same behavior as the core C6 state unless the core is the last one in the package to enter the C7 state. The last core is responsible for flushing the L3 cache. The processor supports the C7s substate, in which the entire L3 cache is flushed in a single step rather than in multiple steps.

The package C-state always resolves the highest power C-state of all of the cores. The package-level power is activated only when all the cores are in low power sleep states.

When all the cores are active, the C-states at the processor package level will be determined by the coordination of C-states as shown in Table 20.

Table 20. Coordination of Core C-states at the package level

Processor states	Coordinated C-states
C0	C0
C1, and no cores are in C0	C1
C3, and no cores are in Co, C1, or C1E	C3
C6, and no cores are in C0, C1, C1E, or C3; or all cores are in C7, but the LLC has not been completed flushed	C6
All cores are in C7 and the LLC has been flushed	C7

Smart battery operation

The system BIOS supports smart battery operation via the ACPI 3.0 Control Method if the smart battery subsystem is present on the carrier board. The smart battery, smart battery manager, smart battery charger, and smart battery selector connect to the PCH's SMBus host controller. For information on the SMBus address on the module used to support smart battery, see *I2C and SMBus on page 42*. Refer to the *Advanced Configuration and Power Interface Specification Revision 4.0* for further information.

Additionally, the sideband signals LID and SLEEP have been added in support of signaling external ACPI power management events for mobile battery-powered applications.

Tips for low power operation

If minimal power consumption is desired, consider making these changes in the BIOS.

- Disable unused interfaces, especially those that consume a lot of power, such as SATA, Ethernet, and PXE.
- Enable Enhanced Intel SpeedStep® technology to reduce the processor frequency and input voltage to the lowest levels supported by the system.
- Enable power saving algorithms.

The following steps are an example of how you can configure the system BIOS to reduce power consumption.

1. During system startup, press <F2> or <Delete> to enter the system setup utility.
2. In the Configuration > Power Control Configuration menu, set RTC Alarm to [Enabled], and set Wake-up Time to a specific time (hour, minute, and second in HH:MM:SS 24-hour clock format).
3. In the Configuration menu, disable the following functions if not required:
   - SATA Operation in the SATA Configuration menu
   - In the USB Configuration menu, set USB Operation to [Disabled].
   - In the PCI Expansion Slot Configuration menu, disable the appropriate ports.
4. If an Ethernet connection is needed but PXE remote boot is not required, make sure that the Ethernet boot device is not selected in the Boot menu's boot priority list.
5. In the Save & Exit menu, choose Save Changes and Restart.

COM Express pinout selection

The COM Express module provides a pinout selection header (J4) to allow you to use either R2.0 Type 6 or R1.0/R2.0 Type 2 pinout definitions for the board-to-board interconnectors. See Figure 1 on page 11 for the header location.

Pinout selection is as follows:

- When a jumper is installed on the header, the COM Express module will use Type 6 pinout definitions.
- When the header is left open, the COM Express module will use Type 2 pinout definitions.

Note: The COM Express module is designed to support a full set of Type 6 features and functionality. When the J4 header is left open to use Type 2 pinout definitions, some features that were defined with standard Type 6 pinouts will become unavailable, such as the legacy PCI and IDE interfaces. Refer to the *COM Express R2.0 Design Guidelines* for further information.

Thermal Solutions

Radisys offers two types of RoHS-compliant thermal solutions:

- Active heatsink
- Heat spreader

Active heatsink

The CEQM67-AHS, shown in Figure 13, is a RoHS-compliant active heatsink that provides up to 80W of thermal dissipation in a chassis that is at least two rack mount units (2U) high. The CEQM67-AHS is used with CEQM77 COM Express modules only.

If you want to use the COM Express module in a 1U chassis, the fan on top of the active heatsink may be removed as long as there is sufficient airflow through the chassis. The required forced airflow across the top of the heatsink in the same direction as the fins is 4 m/s for 60°C ambient temperature.

For assembly instructions, refer to the *Quick Start Guide*.

Figure 13. CEQM67-AHS active heatsink (used with CEQM77)

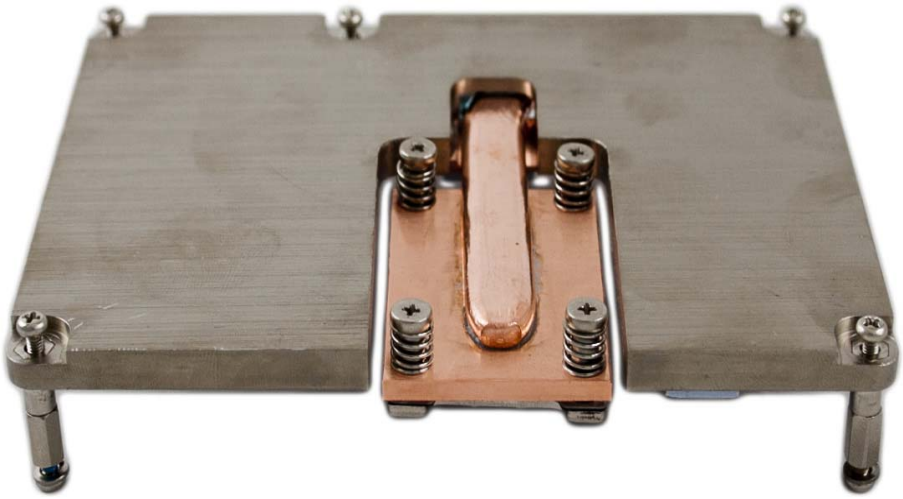
Power requirements

The active heatsink requires an extra +7.0V — +13.2V power supply (+12V recommended). The power connector on the active heatsink is ATX-compliant.

Heat spreader

Radisys also offers a RoHS-compliant heat spreader, CEQM67-77-HSP, which acts as a heat transfer medium to other cooling devices.

Figure 14. CEQM67-77-HSP heat spreader



Mechanical specifications

All dimensions are in millimeters.

Figure 15. CEQM67-AHS heatsink dimensions (bottom view)

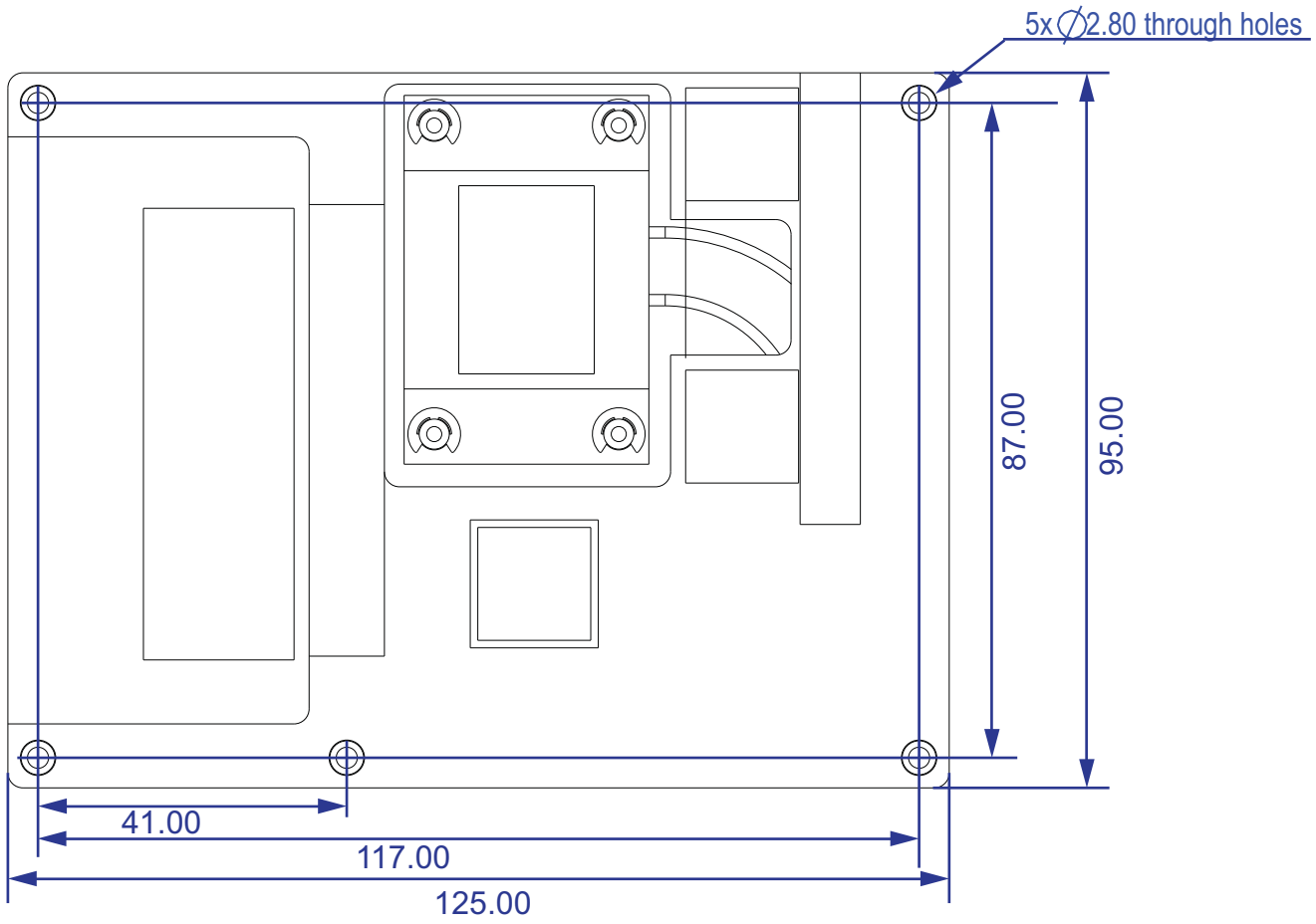


Figure 16. CEQM67-AHS height constraints

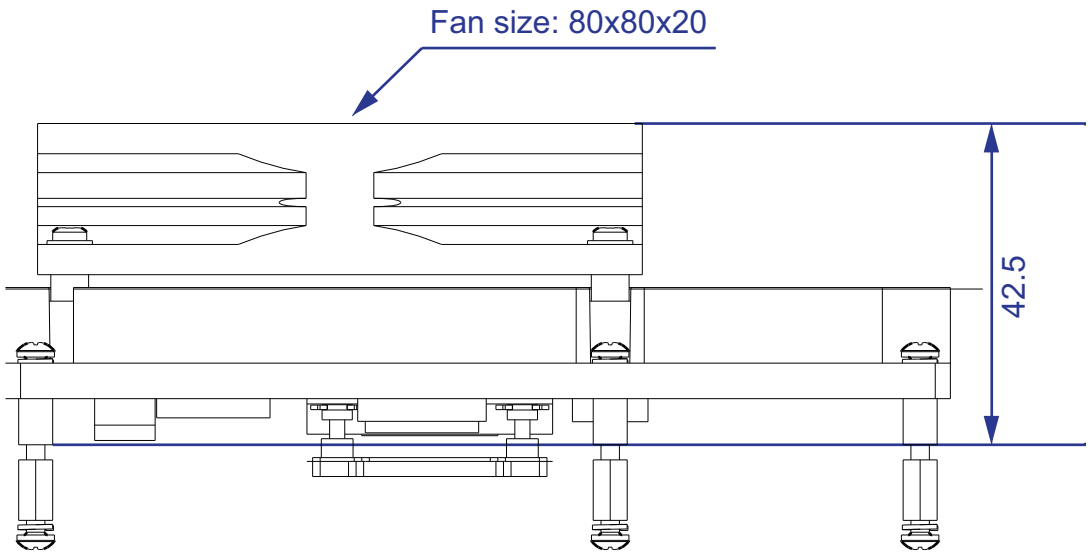


Figure 17. CEQM67-77-HSP heat spreader dimension (bottom view)

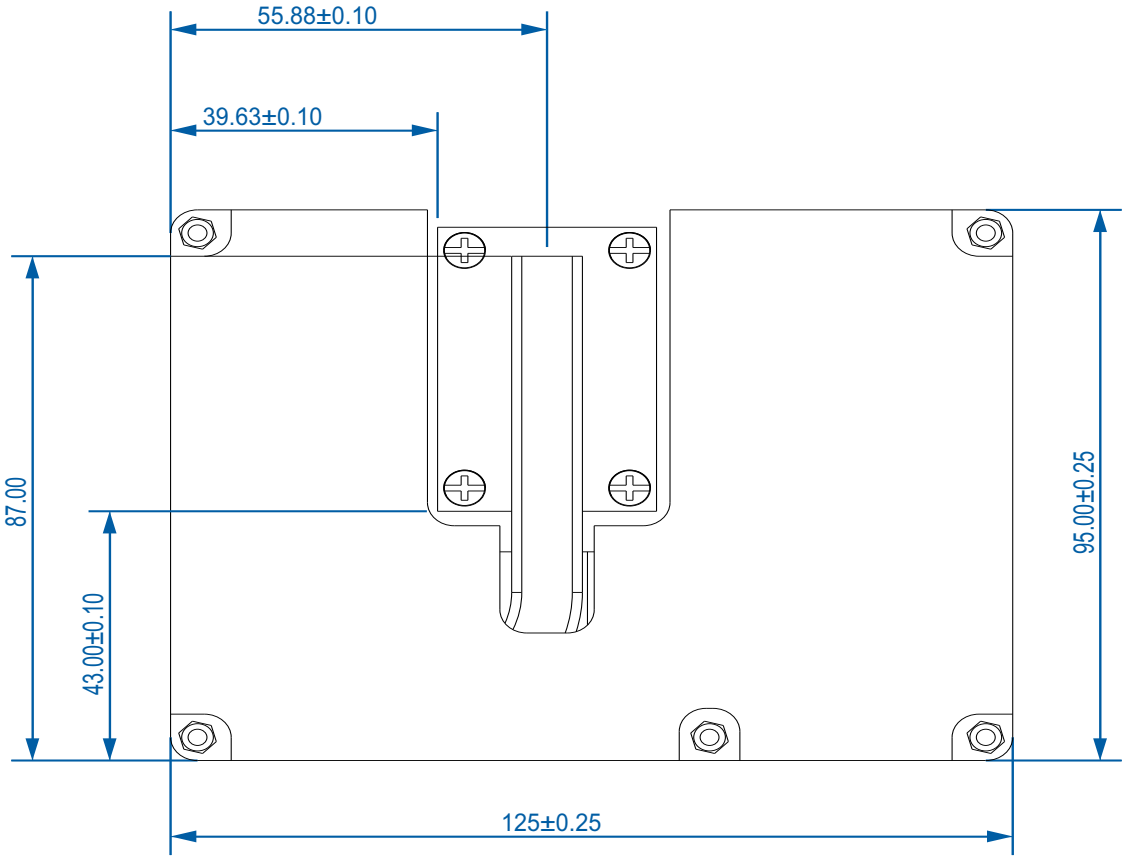
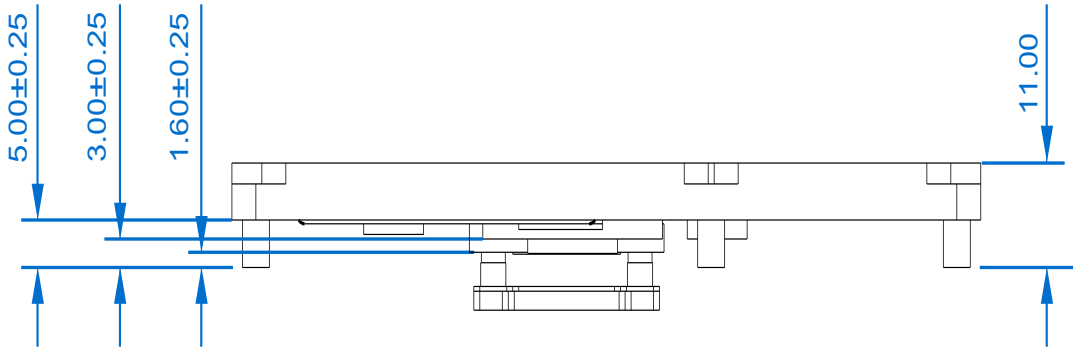


Figure 18. CEQM67-77-HSP height constraints



BIOS Configuration and OS Support

BIOS overview

The system BIOS is based on the AMI® Aptio® Unified Extensible Firmware Interface (UEFI). BIOS features include:

- BIOS readiness for legacy and EFI native operating systems
- Core multi-processing
- ACPI 3.0 wake up events from S3, S4, and S5 power states, including power button, RTC, Wake On LAN, and PME wake up
- Saving and restoration of BIOS configuration settings via the system setup utility
- Automatic detection and BIOS configuration for Winbond® W83627DHG-P, SMSC® SCH3116, SMSC LPC47N217/47N207, Nuvoton® WPCN383U Super I/O legacy devices
- Port 80 Power On Self Test (POST) output to the LPC
- Console redirection to a serial port or USB port 0
- USB 2.0 Debug Port on port 0
- Enhanced Intel SpeedStep technology
- Smart Battery Subsystem management
- Carrier board configuration EEPROM
- Fast boot operation
- High-resolution, GUI-based, customizable splash screen

Using the system setup utility, you can display and modify the system configurations. The BIOS configuration is stored in BIOS flash ROM, and is used to initialize the system.

Boot BIOS selection

Two BIOS boot selection straps, BIOS_DIS[0:1]#, are used to determine whether to boot the system from the SPI BIOS on the module or from the SPI BIOS on the carrier board. The carrier board typically provides jumper selections (or equivalent) to choose the BIOS boot device. For more information on BIOS disable signals, see *SPI flash on page 44*.

For configuration instructions, refer to the carrier board‘s documentation.

POST and boot process

The system BIOS performs a Power On Self Test (POST) upon power-on or reset, which tests and initializes the hardware and programs the chipset and other peripheral components.

When the hardware fails to respond as expected, the POST may not be able to continue. For example, if the memory controller or memory itself cannot be configured, the system cannot continue to initialize the graphics display because the BIOS-level display driver (also known as Video BIOS) requires memory to work properly.

The POST attempts to determine whether further operation is possible. Failures during POST can be indicated with POST codes using a POST card installed on the carrier board's LPC connector. For detailed information, see *Appendix B, POST Messaging, on page 78*.

After POST completes, the system BIOS steps through the boot devices and actions in the configured boot order until the system either loads an operating system successfully or performs a boot action that does not later return to the boot process.

- If a boot device is not operational or not bootable, the system BIOS skips this item. Otherwise, the system BIOS loads the operating system from this boot device and passes control to the operating system. At that point, the system BIOS plays no further part in the boot process except to provide run-time services to the operating system.
- If a boot action is encountered, the system BIOS performs this boot action.
- If the [None] item is reached, the system BIOS enters the system setup utility.

PXE boot

To configure Pre-boot Execution Environment (PXE) boot from Ethernet, see *Configuring PXE boot on page 47* for instructions.

Fast boot

To reduce POST time during system startup, you can remove unnecessary devices and actions from the boot device priority list and/or disable features that are not needed during POST.

Refer to the *Quick Start Guide* for instructions.

Console redirection

To extend video display during system startup, you can use console redirection on USB Port 0 or a module-based serial port. Use the terminal emulation program from AMI to emulate the video display.

Refer to the *Quick Start Guide* for instructions.

Setting up a USB console redirection

By default, the system BIOS is capable of supporting console redirection on the USB Debug Port (USB port 0) and will detect the presence of a USB console automatically.

To set up USB console redirection:

1. Connect a null modem cable from your host computer to a USB port on your carrier board. A USB 2.0 debug cable is required for USB console redirection.
2. Make sure that USB port 0 is enabled in the system setup utility's Configuration > USB Configuration menu.
3. Use a terminal emulation program to emulate the video display, such as the AMI application for USB console redirection.

Setting up a serial console redirection

1. Connect a null modem cable from your host computer to a serial port on your carrier board.
2. During system startup, press <F2> or <Delete> to enter the system setup utility.
3. To set up a console redirection from the serial port on the COM Express module, set Serial Port on Module to [Enabled] on the Configuration > Advanced Configuration menu.
4. In the Configuration > Console Redirection Configuration menu, set Console Redirection to [Enabled] for the desired serial port.
5. In the Console Redirection Settings menu, set the desired console settings.
6. Make sure that you set your host terminal settings to the same values as specified in Step 5.
7. In the Exit menu, save settings and restart.
8. Use a terminal emulation program, such as Windows HyperTerminal, to emulate the video display.

Boot device selection

The system BIOS can start the operating system from any of the following boot devices as long as it is the first bootable device in the Boot Option Priorities list in the system setup utility. Refer to the *Quick Start Guide* for instructions.

- SATA
  - SATA hard disk drive
  - SATA solid state drive
  - SATA CD-ROM/DVD-ROM drive
  - SSDDR module (product option)
- USB
  - USB hard disk drive
  - USB flash drive
  - USB floppy drive
  - USB CD-ROM/DVD-ROM drive
- PXE/Ethernet
- EFI shell

BIOS setup

To enter the system setup utility, press <F2> or <Delete> during system startup. To move through the BIOS menus, use the left and right arrow keys on your keyboard. To move through the BIOS items within a menu, use the up and down arrow keys or press <Tab> and <Shift+Tab>. To select the highlighted item, press <Enter>. To set the value of the selected item, press <+> or <–>. Online help in the system setup screens explains your options for configurable items.

After you have completed the BIOS setup, navigate to the Save & Exit menu to save settings and restart.

For configuration instructions, refer to the *System Setup utility Specification*.

Carrier board serial EEPROM

The system BIOS provides an interface to detect the carrier board serial EEPROM. This is accomplished via the general purpose I^2C interface using board-to-board interconnector pinouts I2C_DAT and I2C_CK. (See *Appendix A, COM Express Module Pinout Definitions, on page 71*.) For more information about the I^2C interface implementation, see *I2C and SMBus on page 42*.

The system BIOS will use any recognizable device information in the EEPROM to set up software-configurable features appropriate for the carrier board. If the EEPROM is incompatible, however, no configuration data will be detected and the BIOS will report an error. Configuration settings in the system setup utility may be changed as a result of this EEPROM detection feature.

Saving and restoring BIOS configurations

Default settings

The SPI BIOS ROM contains a set of standard default BIOS settings. If the NVRAM becomes corrupted, you can restore the default settings to the boot BIOS. This procedure may also be used to revert to the default settings from the current functional settings or user-saved settings.

To restore the default settings, the COM Express module allows you to boot into the BIOS recovery mode by placing a jumper on pins 1 and 2 of the NVRAM Clearing and BIOS Recovery Header (P1). See *Module layout: top view on page 11* for header location. Pin 1 is marked with an asterisk (*) on the PCB.

Note: Removing the RTM battery from the carrier board will reset only the system date and time to their standard default values.

User settings

When you save changes to the BIOS setup utility, BIOS settings are stored in NVRAM. It is possible to change back to the last-saved configuration in NVRAM if the current settings become corrupted.

To restore the last-saved configuration in NVRAM:

1. During system startup, press <F2> or <Delete> to enter the system setup utility.
2. In the Save & Exit menu, select Restore User Defaults.

BIOS update

BIOS release packages are periodically available on the Radisys Web site to address known issues or to add new features. The release packages include instructions for updating the BIOS.

WARNING! BIOS updates should be undertaken with care and only when necessary. If the BIOS update is interrupted by a loss of power before it is complete, the BIOS can be corrupted. Recovery of a corrupted BIOS requires a (USB) recovery disk. Use the instructions provided with the BIOS update to make sure the BIOS update is successful.

BIOS recovery

If the module BIOS becomes corrupted, the COM Express module allows you to boot into the BIOS recovery mode by placing a jumper on pins 2 and 3 of the NVRAM clearing and BIOS recovery header (P1). See *Module layout: top view on page 11* for header location. Pin 1 is marked with an asterisk (*) on the PCB.

You can recover the corrupted BIOS to any functional release rather than the corrupted BIOS image. For detailed instructions, refer to the accompanying recovery readme file in the BIOS release package.

BIOS customization

The system BIOS can be customized with the following components.

- Standard defaults
- Splash screen logos
- Option ROMs
- SLP 2.0 or 2.1 policies
- SMBIOS Type 1, Type 3, and Type 11 information
- PCI Express lane width options

Instructions are provided with the customizing tools. Contact Radisys for information on obtaining these tools.

Additionally, the video BIOS can be customized using the Intel Binary Modification Program utility (*BPM.exe*). This utility is available on the Intel Web site, www.intel.com.

Operating system support

The COM Express module supports the following operating systems. Refer to the *Quick Start Guide* for installation instructions.

- Microsoft Windows 7 (32-bit and 64-bit)
- Ubuntu® Linux 12.04 LTS (32-bit and 64-bit)
- Windows Server 2008 R2 (64-bit)
- Windows Embedded Standard 7 (64-bit)

Drivers and utilities

The operating system you select may require you to install device drivers in order to make the system operational. Visit the Radisys Web site for device drivers and utilities. Refer to the readme files in the release packages for instructions.

COM Express Module Pinout Definitions

The board-to-board interconnector uses a PICMG-compliant 440-pin module receptacle (part number: AMP/Tyco 3-1827231-6 or equivalent), comprising two 220-pin, 0.5mm pitch receptacles (rows A-B and C-D). For information about the module receptacles, refer to *Module interconnectors on page 15*.

Table 21 shows the R2.0 Type 6 pinout definitions that were implemented on the CEQM77 module. The "Design usage" column describes the variations between the module design and the PICMG specification for all product options.

Notes:

- Dashes (—) in the table indicate that the pin definition for the COM Express module is the same as that in the PICMG specification.
- If you are designing a custom carrier board, refer to the *COM Express R2.0 Design Guidelines* for special design instructions.

Table 21. Board-to-board interconnector R2.0 Type 6 pinout definitions

Pin #	PICMG definition	Pin type	Design usage	Pin #	PICMG definition	Pin type	Design usage
A1	GND (FIXED)	GROUND	—	B1	GND (FIXED)	GROUND	—
A2	GBE0_MDI3–	I/O Analog	—	B2	GBE0_ACT#	OD CMOS	—
A3	GBE0_MDI3+	I/O Analog	—	B3	LPC_FRAME#	O CMOS	—
A4	GBE0_LINK100#	OD CMOS	—	B4	LPC_AD0	I/O CMOS	—
A5	GBE0_LINK1000#	OD CMOS	—	B5	LPC_AD1	I/O CMOS	—
A6	GBE0_MDI2–	I/O Analog	—	B6	LPC_AD2	I/O CMOS	—
A7	GBE0_MDI2+	I/O Analog	—	B7	LPC_AD3	I/O CMOS	—
A8	GBE0_LINK#	OD CMOS	—	B8	LPC_DRQ0#	I CMOS	—
A9	GBE0_MDI1–	I/O Analog	—	B9	LPC_DRQ1#	I/O CMOS	—
A10	GBE0_MDI1+	I/O Analog	—	B10	LPC_CLK	O CMOS	—
A11	GND (FIXED)	GROUND	—	B11	GND (FIXED)	GROUND	—
A12	GBE0_MDI0–	I/O Analog	—	B12	PWRBTN#	I CMOS	—
A13	GBE0_MDI0+	I/O Analog	—	B13	SMB_CK	I/O OD CMOS	—
A14	GBE0_CTREF	REF	Refer to the CR300 schematics.	B14	SMB_DAT	I/O OD CMOS	—
A15	SUS_S3#	O CMOS	—	B15	SMB_ALERT#	I CMOS	—
A16	SATA0_TX+	O SATA	—	B16	SATA1_TX+	O SATA	—
A17	SATA0_TX–	O SATA	—	B17	SATA1_TX–	O SATA	—
A18	SUS_S4#	O CMOS	—	B18	SUS_STAT#	O CMOS	—
A19	SATA0_RX+	I SATA	—	B19	SATA1_RX+	I SATA	—
A20	SATA0_RX–	I SATA	—	B20	SATA1_RX–	I SATA	—
A21	GND (FIXED)	GROUND	—	B21	GND (FIXED)	GROUND	—
A22	SATA2_TX+	O SATA	—	B22	SATA3_TX+	O SATA	—

Table 21. Board-to-board interconnector R2.0 Type 6 pinout definitions (continued)

Pin #	PICMG definition	Pin type	Design usage	Pin #	PICMG definition	Pin type	Design usage
A23	SATA2_TX–	O SATA	—	B23	SATA3_TX–	O SATA	—
A24	SUS_S5#	O CMOS	—	B24	PWR_OK	I CMOS	—
A25	SATA2_RX+	I SATA	—	B25	SATA3_RX+	I SATA	—
A26	SATA2_RX–	I SATA	—	B26	SATA3_RX–	I SATA	—
A27	BATLOW#	I CMOS	—	B27	WDT	O CMOS	—
A28	(S)ATA_ACT#	O CMOS	SATA_ACT#	B28	AC/HDA_SDIN2	I CMOS	HDA_SDI2
A29	AC/HDA_SYNC	O CMOS	HDA_SYNC	B29	AC/HDA_SDIN1	I CMOS	HDA_SDI1
A30	AC/HDA_RST#	O CMOS	HDA_RST#	B30	AC/HDA_SDIN0	I CMOS	HDA_SDI0
A31	GND (FIXED)	GROUND	—	B31	GND (FIXED)	GROUND	—
A32	AC/HDA_BITCLK	O CMOS	HDA_CLK	B32	SPKR	O CMOS	—
A33	AC/HDA_SDOUT	O CMOS	HDA_SDO	B33	I2C_CK	O CMOS	—
A34	BIOS_DIS0#	I CMOS	—	B34	I2C_DAT	I/O OD CMOS	—
A35	THRMTRIP#	O CMOS	—	B35	THRM#	I CMOS	—
A36	USB6–	I/O USB	—	B36	USB7–	I/O USB	—
A37	USB6+	I/O USB	—	B37	USB7+	I/O USB	—
A38	USB_6_7_OC#	I CMOS	—	B38	USB_4_5_OC#	I CMOS	—
A39	USB4–	I/O USB	—	B39	USB5–	I/O USB	—
A40	USB4+	I/O USB	—	B40	USB5+	I/O USB	—
A41	GND (FIXED)	GROUND	—	B41	GND (FIXED)	GROUND	—
A42	USB2–	I/O USB	—	B42	USB3–	I/O USB	—
A43	USB2+	I/O USB	—	B43	USB3+	I/O USB	—
A44	USB_2_3_OC#	I CMOS	—	B44	USB_0_1_OC#	I CMOS	—
A45	USB0–	I/O USB	—	B45	USB1–	I/O USB	—
A46	USB0+	I/O USB	—	B46	USB1+	I/O USB	—
A47	VCC_RTC	POWER	—	B47	EXCD1_PERST#	O CMOS	—
A48	EXCD0_PERST#	O CMOS	—	B48	EXCD1_CPPE#	I CMOS	—
A49	EXCD0_CPPE#	I CMOS	—	B49	SYS_RESET#	I CMOS	—
A50	LPC_SERIRQ	I/O CMOS	—	B50	CB_RESET#	O CMOS	—
A51	GND (FIXED)	GROUND	—	B51	GND (FIXED)	GROUND	—
A52	PCIE_TX5+	O PCIE	—	B52	PCIE_RX5+	I PCIE	—
A53	PCIE_TX5–	O PCIE	—	B53	PCIE_RX5–	I PCIE	—
A54	GPI0	I CMOS	—	B54	GPO1	O CMOS	—
A55	PCIE_TX4+	O PCIE	—	B55	PCIE_RX4+	I PCIE	—
A56	PCIE_TX4–	O PCIE	—	B56	PCIE_RX4–	I PCIE	—
A57	GND	GROUND	—	B57	GPO2	O CMOS	—
A58	PCIE_TX3+	O PCIE	—	B58	PCIE_RX3+	I PCIE	—
A59	PCIE_TX3–	O PCIE	—	B59	PCIE_RX3–	I PCIE	—
A60	GND (FIXED)	GROUND	—	B60	GND (FIXED)	GROUND	—
A61	PCIE_TX2+	O PCIE	—	B61	PCIE_RX2+	I PCIE	—
A62	PCIE_TX2–	O PCIE	—	B62	PCIE_RX2–	I PCIE	—

Table 21. Board-to-board interconnector R2.0 Type 6 pinout definitions (continued)

Pin #	PICMG definition	Pin type	Design usage	Pin #	PICMG definition	Pin type	Design usage
A63	GPI1	I CMOS	—	B63	GPO3	O CMOS	—
A64	PCIE_TX1+	O PCIE	—	B64	PCIE_RX1+	I PCIE	—
A65	PCIE_TX1–	O PCIE	—	B65	PCIE_RX1–	I PCIE	—
A66	GND	GROUND	—	B66	WAKE0#	I CMOS	—
A67	GPI2	I CMOS	GPI2/ICCMON	B67	WAKE1#	I CMOS	—
A68	PCIE_TX0+	O PCIE	—	B68	PCIE_RX0+	I PCIE	—
A69	PCIE_TX0–	O PCIE	—	B69	PCIE_RX0–	I PCIE	—
A70	GND (FIXED)	GROUND	—	B70	GND (FIXED)	GROUND	—
A71	LVDS_A0+	O LVDS	—	B71	LVDS_B0+	O LVDS	—
A72	LVDS_A0–	O LVDS	—	B72	LVDS_B0–	O LVDS	—
A73	LVDS_A1+	O LVDS	—	B73	LVDS_B1+	O LVDS	—
A74	LVDS_A1–	O LVDS	—	B74	LVDS_B1–	O LVDS	—
A75	LVDS_A2+	O LVDS	—	B75	LVDS_B2+	O LVDS	—
A76	LVDS_A2–	O LVDS	—	B76	LVDS_B2–	O LVDS	—
A77	LVDS_VDD_EN	O LVDS	—	B77	LVDS_B3+	O LVDS	—
A78	LVDS_A3+	O LVDS	—	B78	LVDS_B3–	O LVDS	—
A79	LVDS_A3–	O LVDS	—	B79	LVDS_BKLT_EN	O LVDS	—
A80	GND (FIXED)	GROUND	—	B80	GND (FIXED)	GROUND	—
A81	LVDS_A_CK+	O LVDS	—	B81	LVDS_B_CK+	O LVDS	—
A82	LVDS_A_CK–	O LVDS	—	B82	LVDS_B_CK–	O LVDS	—
A83	LVDS_I2C_CK	O LVDS	—	B83	LVDS_BKLT_CTRL	O CMOS	—
A84	LVDS_I2C_DAT	O LVDS	—	B84	VCC_5V_SBY	POWER	—
A85	GPI3	I CMOS	GPI3/ACPRESENT	B85	VCC_5V_SBY	POWER	—
A86	RSVD	I CMOS	RSVD	B86	VCC_5V_SBY	POWER	—
A87	RSVD	I CMOS	RSVD	B87	VCC_5V_SBY	POWER	—
A88	PCIE_CLK_REF+	O PCIE	—	B88	BIOS_DIS1#	I CMOS	—
A89	PCIE_CK_REF–	O CMOS	—	B89	VGA_RED	O Analog	—
A90	GND (FIXED)	GROUND	—	B90	GND (FIXED)	GROUND	—
A91	SPI_POWER	O POWEr	—	B91	VGA_GRN	O Analog	—
A92	SPI_MISO	I CMOS	—	B92	VGA_BLU	O Analog	—
A93	GPO0	O CMOS	—	B93	VGA_HSYNC	O CMOS	—
A94	SPI_CLK	O CMOS	—	B94	VGA_VSYNC	O CMOS	—
A95	SPI_MOSI	O CMOS	—	B95	VGA_I2C_CK	O CMOS	—
A96	TPM_PP	I CMOS	—	B96	VGA_I2C_DAT	I/O OD CMOS	—
A97	TYPE10#	PDS	Not connected	B97	SPI_CS#	O CMOS	—
A98	SER0_TX	O CMOS	—	B98	RSVD	RSVD	Not connected
A99	SER0_RX	I CMOS	—	B99	RSVD	RSVD	Not connected
A100	GND (FIXED)	GROUND	—	B100	GND (FIXED)	GROUND	—
A101	SER1_TX	O CMOS	Not connected	B101	FAN_PWMOUT	O OD CMOS	—
A102	SER1_RX	I CMOS	Not connected	B102	FAN_TACHIN	I OD CMOS	—

Table 21. Board-to-board interconnector R2.0 Type 6 pinout definitions (continued)

Pin #	PICMG definition	Pin type	Design usage	Pin #	PICMG definition	Pin type	Design usage
A103	LID#	I OD CMOS	—	B103	SLEEP#	I OD CMOS	—
A104	VCC_12V	POWER	—	B104	VCC_12V	POWER	—
A105	VCC_12V	POWER	—	B105	VCC_12V	POWER	—
A106	VCC_12V	POWER	—	B106	VCC_12V	POWER	—
A107	VCC_12V	POWER	—	B107	VCC_12V	POWER	—
A108	VCC_12V	POWER	—	B108	VCC_12V	POWER	—
A109	VCC_12V	POWER	—	B109	VCC_12V	POWER	—
A110	GND (FIXED)	GROUND	—	B110	GND (FIXED)	GROUND	—
C1	GND (FIXED)	GROUND	—	D1	GND (FIXED)	GROUND	—
C2	GND	GROUND	—	D2	GND	GROUND	—
C3	USB_SSRX0–	I PCIE	—	D3	USB_SSTX0–	O PCIE	—
C4	USB_SSRX0+	I PCIE	—	D4	USB_SSTX0+	O PCIE	—
C5	GND	GROUND	—	D5	GND	GROUND	—
C6	USB_SSRX1–	I PCIE	—	D6	USB_SSTX1–	O PCIE	—
C7	USB_SSRX1+	I PCIE	—	D7	USB_SSTX1+	O PCIE	—
C8	GND	GROUND	—	D8	GND	GROUND	—
C9	USB_SSRX2–	I PCIE	—	D9	USB_SSTX2–	O PCIE	—
C10	USB_SSRX2+	I PCIE	—	D10	USB_SSTX2+	O PCIE	—
C11	GND (FIXED)	GROUND	—	D11	GND (FIXED)	GROUND	—
C12	USB_SSRX3–	I PCIE	—	D12	USB_SSTX3–	O PCIE	—
C13	USB_SSRX3+	I PCIE	—	D13	USB_SSTX3+	O PCIE	—
C14	GND	GROUND	—	D14	GND	GROUND	—
C15	DDI1_PAIR6+	O PCIE	SDVO_STALL+	D15	DDI1_CTRLCLK_AUX+	I/O PCIE	—
C16	DDI1_PAIR6–	O PCIE	SDVO_STALL–	D16	DDI1_CTRLDATA_AUX–	I/O PCIE	—
C17	RSVD	RSVD	Not connected	D17	RSVD	RSVD	Not connected
C18	RSVD	RSVD	Not connected	D18	RSVD	RSVD	Not connected
C19	PCIE_RX6+	I PCIE	—	D19	PCIE_TX6+	O PCIE	—
C20	PCIE_RX6–	I PCIE	—	D20	PCIE_TX6–	O PCIE	—
C21	GND (FIXED)	GROUND	—	D21	GND (FIXED)	GROUND	—
C22	PCIE_RX7+	I PCIE	Not connected	D22	PCIE_TX7+	O PCIE	Not connected
C23	PCIE_RX7–	I PCIE	Not connected	D23	PCIE_TX7–	O PCIE	Not connected
C24	DDI1_HPD	IO CMOS	—	D24	RSVD	RSVD	Not connected
C25	DDI1_PAIR4+	IO CMOS	SDVO_INT+	D25	RSVD	RSVD	Not connected
C26	DDI1_PAIR4–	IO CMOS	SDVO_INT–	D26	DDI1_PAIR0+	O PCIE	—
C27	RSVD	RSVD	Not connected	D27	DDI1_PAIR0–	O PCIE	—
C28	RSVD	RSVD	Not connected	D28	RSVD	RSVD	Not connected
C29	DDI1_PAIR5+	IO CMOS	SDVO_TVCLKIN+	D29	DDI1_PAIR1+	O PCIE	—
C30	DDI1_PAIR5–	IO CMOS	SDVO_TVCLKIN+	D30	DDI1_PAIR1–	O PCIE	—

Table 21. Board-to-board interconnector R2.0 Type 6 pinout definitions (continued)

Pin #	PICMG definition	Pin type	Design usage	Pin #	PICMG definition	Pin type	Design usage
C31	GND (FIXED)	GROUND	—	D31	GND (FIXED)	GROUND	—
C32	DDI2_CTRLCLK_ AUX+	I/O CMOS	—	D32	DDI1_PAIR2+	O PCIE	—
C33	DDI2_CTRLDATA_ AUX–	I/O CMOS	—	D33	DDI1_PAIR2–	O PCIE	—
C34	DDI2_DDC_AUX_SEL	I/O CMOS	—	D34	DDI1_DDC_AUX_SEL	IO OD CMOS	—
C35	RSVD	RSVD	Not connected	D35	RSVD	RSVD	Not connected
C36	DDI3_CTRLCLK_ AUX+	I/O CMOS	—	D36	DDI1_PAIR3+	O PCIE	—
C37	DDI3_CTRLDATA_ AUX–	I/O CMOS	—	D37	DDI1_PAIR3–	O PCIE	—
C38	DDI3_DDC_AUX_SEL	I/O CMOS	—	D38	RSVD	RSVD	—
C39	DDI3_PAIR0+	I/O CMOS	—	D39	DDI2_PAIR0+	O PCIE	—
C40	DDI3_PAIR0–	I/O CMOS	—	D40	DDI2_PAIR0–	O PCIE	—
C41	GND (FIXED)	GROUND	—	D41	GND (FIXED)	GROUND	—
C42	DDI3_PAIR1+	I PCIE	—	D42	DDI2_PAIR1+	O PCIE	—
C43	DDI3_PAIR1–	I PCIE	—	D43	DDI2_PAIR1–	O PCIE	—
C44	DDI3_HPD	I CMOS	—	D44	DDI2_HPD	I CMOS	—
C45	RSVD	I CMOS	Not connected	D45	RSVD	RSVD	Not connected
C46	DDI3_PAIR2+	I PCIE	—	D46	DDI2_PAIR2+	O PCIE	—
C47	DDI3_PAIR2–	I PCIE	—	D47	DDI2_PAIR2–	O PCIE	—
C48	RSVD	RSVD	Not connected	D48	RSVD	RSVD	Not connected
C49	DDI3_PAIR3+	I PCIE	—	D49	DDI2_PAIR3+	O PCIE	—
C50	DDI3_PAIR3–	I PCIE	—	D50	DDI2_PAIR3–	O PCIE	—
C51	GND (FIXED)	GROUND	—	D51	GND (FIXED)	GROUND	—
C52	PEG_RX0+	I PCIE	—	D52	PEG_TX0+	O PCIE	—
C53	PEG_RX0–	I PCIE	—	D53	PEG_TX0–	O PCIE	—
C54	TYPE0#	PDS	Not connected	D54	PEG_LANE_RV#	I CMOS	—
C55	PEG_RX1+	I PCIE	—	D55	PEG_TX1+	O PCIE	—
C56	PEG_RX1–	I PCIE	—	D56	PEG_TX1–	O PCIE	—
C57	TYPE1#	PDS	Not connected	D57	TYPE2#	PDS	—
C58	PEG_RX2+	I PCIE	—	D58	PEG_TX2+	O PCIE	—
C59	PEG_RX2–	I PCIE	—	D59	PEG_TX2–	O PCIE	—
C60	GND (FIXED)	GROUND	—	D60	GND (FIXED)	GROUND	—
C61	PEG_RX3+	I PCIE	—	D61	PEG_TX3+	O PCIE	—
C62	PEG_RX3–	I PCIE	—	D62	PEG_TX3–	O PCIE	—
C63	RSVD	RSVD	Not connected	D63	RSVD	RSVD	Not connected
C64	RSVD	RSVD	Not connected	D64	RSVD	RSVD	Not connected
C65	PEG_RX4+	I PCIE	—	D65	PEG_TX4+	O PCIE	—
C66	PEG_RX4–	I PCIE	—	D66	PEG_TX4–	O PCIE	—

Table 21. Board-to-board interconnector R2.0 Type 6 pinout definitions (continued)

Pin #	PICMG definition	Pin type	Design usage	Pin #	PICMG definition	Pin type	Design usage
C67	RSVD	RSVD	Not connected	D67	GND	GROUND	—
C68	PEG_RX5+	I PCIE	—	D68	PEG_TX5+	O PCIE	—
C69	PEG_RX5–	I PCIE	—	D69	PEG_TX5–	O PCIE	—
C70	GND (FIXED)	GROUND	—	D70	GND (FIXED)	GROUND	—
C71	PEG_RX6+	I PCIE	—	D71	PEG_TX6+	O PCIE	—
C72	PEG_RX6–	I PCIE	—	D72	PEG_TX6–	O PCIE	—
C73	GND (FIXED)	GROUND	—	D73	GND (FIXED)	GROUND	Not connected
C74	PEG_RX7+	I PCIE	—	D74	PEG_TX7+	O PCIE	—
C75	PEG_RX7–	I PCIE	—	D75	PEG_TX7–	O PCIE	—
C76	GND	GROUND	—	D76	GND	GROUND	—
C77	RSVD	RSVD	Not connected	D77	RSVD	RSVD	Not connected
C78	PEG_RX8+	I PCIE	—	D78	PEG_TX8+	O PCIE	—
C79	PEG_RX8–	I PCIE	—	D79	PEG_TX8–	O PCIE	—
C80	GND (FIXED)	GROUND	—	D80	GND (FIXED)	GROUND	—
C81	PEG_RX9+	I PCIE	—	D81	PEG_TX9+	O PCIE	—
C82	PEG_RX9–	I PCIE	—	D82	PEG_TX9–	O PCIE	—
C83	RSVD	RSVD	Not connected	D83	RSVD	RSVD	Not connected
C84	GND	GROUND	—	D84	GND	GROUND	—
C85	PEG_RX10+	I PCIE	—	D85	PEG_TX10+	O PCIE	—
C86	PEG_RX10–	I PCIE	—	D86	PEG_TX10–	O PCIE	—
C87	GND	GROUND		D87	GND	GROUND	—
C88	PEG_RX11+	I PCIE	—	D88	PEG_TX11+	O PCIE	—
C89	PEG_RX11–	I PCIE	—	D89	PEG_TX11–	O PCIE	—
C90	GND (FIXED)	GROUND		D90	GND (FIXED)	GROUND	—
C91	PEG_RX12+	I PCIE	—	D91	PEG_TX12+	O PCIE	—
C92	PEG_RX12–	I PCIE	—	D92	PEG_TX12–	O PCIE	—
C93	GND	GROUND	—	D93	GND	GROUND	—
C94	PEG_RX13+	I PCIE	—	D94	PEG_TX13+	O PCIE	—
C95	PEG_RX13–	I PCIE	—	D95	PEG_TX13–	O PCIE	—
C96	GND	GROUND	—	D96	GND	GROUND	—
C97	RSVD	RSVD	Not connected	D97	RSVD	I CMOS	—
C98	PEG_RX14+	I PCIE	—	D98	PEG_TX14+	O PCIE	—
C99	PEG_RX14–	I PCIE	—	D99	PEG_TX14–	O PCIE	—
C100	GND (FIXED)	GROUND		D100	GND (FIXED)	GROUND	—
C101	PEG_RX15+	I PCIE	—	D101	PEG_TX15+	O PCIE	—
C102	PEG_RX15–	I PCIE	—	D102	PEG_TX15–	O PCIE	—
C103	GND	GROUND	—	D103	GND	GROUND	—
C104	VCC_12V	POWER	Module primary power input from carrier	D104	VCC_12V	POWER	Module primary power input from carrier

Table 21. Board-to-board interconnector R2.0 Type 6 pinout definitions (continued)

Pin #	PICMG definition	Pin type	Design usage	Pin #	PICMG definition	Pin type	Design usage
C105	VCC_12V	POWER	Module primary power input from carrier	D105	VCC_12V	POWER	Module primary power input from carrier
C106	VCC_12V	POWER	Module primary power input from carrier	D106	VCC_12V	POWER	Module primary power input from carrier
C107	VCC_12V	POWER	Module primary power input from carrier	D107	VCC_12V	POWER	Module primary power input from carrier
C108	VCC_12V	POWER	Module primary power input from carrier	D108	VCC_12V	POWER	Module primary power input from carrier
C109	VCC_12V	POWER	Module primary power input from carrier	D109	VCC_12V	POWER	Module primary power input from carrier
C110	GND (FIXED)	GROUND	—	D110	GND (FIXED)	GROUND	—

POST Messaging

The system BIOS tests and initializes the hardware during POST. If the hardware fails to respond as expected before the system is sufficiently operational to display messages on the screen, the BIOS will use Port80 POST codes to indicate critical problems. If no POST code card is available, the BIOS uses the system speaker to signal a problem with beeps.

The Intel Platform Innovation Framework for EFI defines four *boot phases*:

- Security (SEC): initial low-level initialization
- Pre-EFI Initialization (PEI): memory initialization
- Driver Execution Environment (DXE): main hardware initialization
- Boot Device Selection (BDS): system setup, pre-OS user interface, and selection of bootable device

POST codes

POST codes are typically sent to I/O port 0x80, but the Aptio core will send codes to the LPC bus.

Table 22. Status code ranges

Status code range	Description
0x01–0x0F	SEC Status Codes & Errors
0x10–0x2F	PEI execution up to and including memory detection
0x30–0x4F	PEI execution after memory detection
0x50–0x5F	PEI errors
0x60–0xCF	DXE execution up to BDS
0xD0–0xDF	DXE errors
0xE0–0xE8	S3 Resume (PEI)
0xE9–0xEF	S3 Resume errors (PEI)
0xF0–0xF8	Recovery (PEI)
0xF9–0xFF	Recovery errors (PEI)

Table 23 through Table 27 provide a reference for diagnosing problems in booting.

Table 23. SEC status codes

Status code range	Description
0x0	Not used
0x1	Power on. Reset type detection (soft/hard).
0x2	AP initialization before microcode loading
0x3	North Bridge initialization before microcode loading
0x4	South Bridge initialization before microcode loading
0x5	OEM initialization before microcode loading
0x6	Microcode loading
0x7	AP initialization after microcode loading
0x8	North Bridge initialization after microcode loading
0x9	South Bridge initialization after microcode loading
0xA	OEM initialization after microcode loading
0xB	Cache initialization
SEC Error Codes	
0xC–0xD	Reserved for future AMI SEC error codes
0xE	Microcode not found
0xF	Microcode not loaded

Table 24. PEI Status Codes

Status code	Description
0x10	PEI core has started
0x11	Pre-memory CPU initialization has started
0x12	Pre-memory CPU initialization (CPU module specific)
0x13	Pre-memory CPU initialization (CPU module specific)
0x14	Pre-memory CPU initialization (CPU module specific)
0x15	Pre-memory North Bridge initialization has started
0x16	Pre-Memory North Bridge initialization (North Bridge module specific)
0x17	Pre-Memory North Bridge initialization (North Bridge module specific)
0x18	Pre-Memory North Bridge initialization (North Bridge module specific)
0x19	Pre-memory South Bridge initialization has started
0x1A	Pre-memory South Bridge initialization (South Bridge module specific)
0x1B	Pre-memory South Bridge initialization (South Bridge module specific)
0x1C	Pre-memory South Bridge initialization (South Bridge module specific)
0x1D–0x2A	OEM pre-memory initialization codes
0x2B	Memory initialization. Serial Presence Detect (SPD) data reading
0x2C	Memory initialization. Memory presence detection
0x2D	Memory initialization. Programming memory timing information
0x2E	Memory initialization. Configuring memory
0x2F	Memory initialization (other).

Table 24. PEI Status Codes (continued)

Status code	Description
0x30	Reserved for ASL (see ASL Status Codes section below)
0x31	Memory Installed
0x32	CPU post-memory initialization has started
0x33	CPU post-memory initialization. Cache initialization
0x34	CPU post-memory initialization. Application Processor(s) (AP) initialization
0x35	CPU post-memory initialization. Boot Strap Processor (BSP) selection
0x36	CPU post-memory initialization. System Management Mode (SMM) initialization
0x37	Post-Memory North Bridge initialization has started
0x38	Post-Memory North Bridge initialization (North Bridge module specific)
0x39	Post-Memory North Bridge initialization (North Bridge module specific)
0x3A	Post-Memory North Bridge initialization (North Bridge module specific)
0x3B	Post-Memory South Bridge initialization has started
0x3C	Post-Memory South Bridge initialization (South Bridge module specific)
0x3D	Post-Memory South Bridge initialization (South Bridge module specific)
0x3E	Post-Memory South Bridge initialization (South Bridge module specific)
0x3F–0x4E	OEM post memory initialization codes
0x4F	DXE IPL has started
PEI Error Codes	
0x50	Memory initialization error. Invalid memory type or incompatible memory speed
0x51	Memory initialization error. SPD reading has failed
0x52	Memory initialization error. Invalid memory size or memory modules do not match.
0x53	Memory initialization error. No usable memory detected
0x54	Unspecified memory initialization error.
0x55	Memory not installed
0x56	Invalid CPU type or Speed
0x57	CPU mismatch
0x58	CPU self test failed or possible CPU cache error
0x59	CPU micro-code is not found or micro-code update has failed
0x5A	Internal CPU error
0x5B	reset PPI is not available
0x5C–0x5F	Reserved for future AMI error codes
S3 Resume Progress Codes	
0xE0	S3 Resume has stared (S3 Resume PPI is called by the DXE IPL)
0xE1	S3 Boot Script execution
0xE2	Video repost
0xE3	OS S3 wake vector call
0xE4–0xE7	Reserved for future AMI progress codes
0xE0	S3 Resume has started (S3 Resume PPI is called by the DXE IPL)
S3 Resume Error Codes	
0xE8	S3 Resume Failed in PEI

Table 24. PEI Status Codes (continued)

Status code	Description
0xE9	S3 Resume PPI not Found
0xEA	S3 Resume Boot Script Error
0xEB	S3 OS Wake Error
0xEC–0xEF	Reserved for future AMI error codes
Recovery Progress Codes	
0xF0	Recovery condition triggered by firmware (Auto recovery)
0xF1	Recovery condition triggered by user (Forced recovery)
0xF2	Recovery process started
0xF3	Recovery firmware image has been found
0xF4	Recovery firmware image is loaded
0xF5–0xF7	Reserved for future AMI progress codes
Recovery Error Codes	
0xF8	Recovery PPI is not available
0xF9	Recovery capsule is not found
0xFA	Invalid recovery capsule
0xFB–0xFF	Reserved for future AMI error codes

Table 25. DXE status codes

Status Code	Description
0x60	DXE Core has started
0x61	NVRAM initialization
0x62	Installation of the South Bridge Runtime Services
0x63	CPU DXE initialization has started
0x64	CPU DXE initialization (CPU module specific)
0x65	CPU DXE initialization (CPU module specific)
0x66	CPU DXE initialization (CPU module specific)
0x67	CPU DXE initialization (CPU module specific)
0x68	PCI host bridge initialization
0x69	North Bridge DXE initialization has started
0x6A	North Bridge DXE SMM initialization has started
0x6B	North Bridge DXE initialization (North Bridge module specific)
0x6C	North Bridge DXE initialization (North Bridge module specific)
0x6D	North Bridge DXE initialization (North Bridge module specific)
0x6E	North Bridge DXE initialization (North Bridge module specific)
0x6F	North Bridge DXE initialization (North Bridge module specific)
0x70	South Bridge DXE initialization has started
0x71	South Bridge DXE SMM initialization has started
0x72	South Bridge devices initialization
0x73	South Bridge DXE Initialization (South Bridge module specific)
0x74	South Bridge DXE Initialization (South Bridge module specific)

Table 25. DXE status codes (continued)

Status Code	Description
0x75	South Bridge DXE Initialization (South Bridge module specific)
0x76	South Bridge DXE Initialization (South Bridge module specific)
0x77	South Bridge DXE Initialization (South Bridge module specific)
0x78	ACPI module initialization
0x79	CSM initialization
0x7A–0x7F	Reserved for future AMI DXE codes
0x80–0x8F	OEM DXE initialization codes
0x90	Boot Device Selection (BDS) phase has started
0x91	Driver connecting has started
0x92	PCI Bus initialization has started
0x93	PCI Bus Hot Plug Controller Initialization
0x94	PCI Bus Enumeration
0x95	PCI Bus Request Resources
0x96	PCI Bus Assign Resources
0x97	Console Output devices connect
0x98	Console input devices connect
0x99	Super IO Initialization
0x9A	USB initialization has started
0x9B	USB Reset
0x9C	USB Detect
0x9D	USB Enable
0x9E–0x9F	Reserved for future AMI codes
0xA0	IDE initialization has started
0xA1	IDE Reset
0xA2	IDE Detect
0xA3	IDE Enable
0xA4	SCSI initialization has started
0xA5	SCSI Reset
0xA6	SCSI Detect
0xA7	SCSI Enable
0xA8	Setup Verifying Password
0xA9	Start of Setup
0xAA	Reserved for ASL (see ASL Status Codes section below)
0xAB	Setup Input Wait
0xAC	Reserved for ASL (see ASL Status Codes section below)
0xAD	Ready To Boot event
0xAE	Legacy Boot event
0xAF	Exit Boot Services event
0xB0	Runtime Set Virtual Address MAP Begin
0xB1	Runtime Set Virtual Address MAP End

Table 25. DXE status codes (continued)

Status Code	Description
0xB2	Legacy Option ROM Initialization
0xB3	System Reset
0xB4	USB hot plug
0xB5	PCI bus hot plug
0xB6	Clean-up of NVRAM
0xB7	Configuration Reset (reset of NVRAM settings)
0xB8–0xBF	Reserved for future AMI codes
0xC0–0xCF	OEM BDS initialization codes
DXE Error Codes	
0xD0	CPU initialization error
0xD1	North Bridge initialization error
0xD2	South Bridge initialization error
0xD3	Some of the Architectural Protocols are not available
0xD4	PCI resource allocation error. Out of Resources
0xD5	No Space for Legacy Option ROM
0xD6	No Console Output Devices are found
0xD7	No Console Input Devices are found
0xD8	Invalid password
0xD9	Error loading Boot Option (LoadImage returned error)
0xDA	Boot Option has failed (StartImage returned error)
0xDB	Flash update has failed
0xDC	Reset protocol is not available

Table 26. ASL status codes

Status Code Range	Description
0x01	System is entering S1 sleep state
0x02	Systejtm is entering S2 sleep state
0x03	System is entering S3 sleep state
0x04	System is entering S4 sleep state
0x05	System is entering S5 sleep state
0x10	System is waking up from the S1 sleep state
0x20	System is waking up from the S2 sleep state
0x30	System is waking up from the S3 sleep state
0x40	System is waking up from the S4 sleep state
0xAC	System has transitioned into ACPI mode. Interrupt controller is in PIC mode
0xAA	System has transitioned into ACPI mode. Interrupt controller is in APIC mode

Table 27. OEM-reserved status code ranges

Status Code Range	Description
0x5	OEM SEC initialization before microcode loading
0xA	OEM SEC initialization after microcode loading
0x1D–0x2A	OEM pre-memory initialization codes
0x3F–0x4E	OEM PEI post memory initialization codes
0x80–0x8F	OEM DXE initialization codes
0xC0–0xCF	OEM BDS initialization codes

Beep codes

Table 28. PEI beep codes

Beeps	Description
1	Memory not Installed
1	Memory was installed twice (InstallPeiMemory routine in PEI Core called twice)
2	Recovery started
3	DXEIPL was not found
3	DXE Core Firmware Volume was not found
7	Reset PPI is not available
4	Recovery failed
4	S3 Resume failed

Table 29. DXE beep codes

Beeps	Description
4	Some of the Architectural Protocols are not available
5	No Console Output Devices are found
5	No Console Input Devices are found
1	Invalid password
6	Flash update has failed
7	Reset protocol is not available
8	Platform PCI resource requirements cannot be met