

# » Kontron User's Guide «



## COMe-bHL6

Document Revision 2.2

This page has been intentionally left blank

# » Table of Contents «

|          |   |           |
|----------|---|-----------|
| <b>1</b> | <b><u>User Information</u></b> .....                                | <b>6</b>  |
| 1.1      | <u>Revision History</u> .....                                       | 6         |
| 1.2      | <u>About This Document</u> .....                                    | 6         |
| 1.3      | <u>Copyright Notice</u> .....                                       | 6         |
| 1.4      | <u>Trademarks</u> .....   | 6         |
| 1.5      | <u>Standards</u> .....  | 6         |
| 1.6      | <u>Warranty</u> .....   | 7         |
| 1.7      | <u>Technical Support</u> .....                                      | 7         |
| <b>2</b> | <b><u>Introduction</u></b> .....                                    | <b>8</b>  |
| 2.1      | <u>Product Description</u> .....                                    | 8         |
| 2.2      | <u>Naming clarification</u> .....                                   | 8         |
| 2.3      | <u>Understanding COM Express® Functionality</u> .....               | 9         |
| 2.4      | <u>COM Express® Documentation</u> .....                             | 10        |
| 2.5      | <u>COM Express® Benefits</u> .....                                  | 10        |
| <b>3</b> | <b><u>Product Specification</u></b> .....                           | <b>11</b> |
| 3.1      | <u>Module definition</u> .....                                      | 11        |
| 3.2      | <u>Functional Specification</u> .....                               | 12        |
| 3.3      | <u>Block Diagram</u> .....  | 21        |
| 3.4      | <u>Accessories</u> .....  | 22        |
| 3.5      | <u>Electrical Specification</u> .....                               | 23        |
| 3.5.1    | <u>Supply Voltage</u> .....   | 23        |
| 3.5.2    | <u>Power Supply Rise Time</u> .....                                 | 23        |
| 3.5.3    | <u>Supply Voltage Ripple</u> .....                                  | 23        |
| 3.5.4    | <u>Power Consumption</u> .....                                      | 23        |
| 3.5.5    | <u>ATX Mode</u> .....   | 24        |
| 3.5.6    | <u>Single Supply Mode</u> .....                                     | 24        |
| 3.6      | <u>Power Control</u> .....  | 25        |
| 3.7      | <u>Environmental Specification</u> .....                            | 26        |
| 3.7.1    | <u>Temperature Specification</u> .....                              | 26        |
| 3.7.2    | <u>Humidity</u> .....   | 26        |
| 3.8      | <u>Standards and Certifications</u> .....                           | 27        |
| 3.9      | <u>MTBF</u> .....   | 29        |
| 3.10     | <u>Mechanical Specification</u> .....                               | 30        |
| 3.11     | <u>Module Dimensions</u> .....                                      | 31        |
| 3.12     | <u>Thermal Management, Heatspreader and Cooling Solutions</u> ..... | 32        |
| 3.13     | <u>Onboard Connectors</u> .....                                     | 33        |
| 3.13.1   | <u>FAN Connector J6 - PCB bottom</u> .....                          | 33        |
| 3.13.2   | <u>CPU JTAG connector J3 - PCB bottom</u> .....                     | 34        |
| 3.13.3   | <u>CPLD Debug connector J7 - PCB top</u> .....                      | 34        |
| <b>4</b> | <b><u>Features and Interfaces</u></b> .....                         | <b>35</b> |
| 4.1      | <u>S5 Eco Mode</u> .....  | 35        |

|          |  |           |
|----------|--|-----------|
| 4.2      | <a href="#">Rapid Shutdown</a> .....                                       | 36        |
| 4.3      | <a href="#">LPC</a> .....  | 38        |
| 4.4      | <a href="#">Serial Peripheral Interface (SPI)</a> .....                    | 39        |
| 4.5      | <a href="#">SPI boot</a> .....   | 39        |
| 4.6      | <a href="#">M.A.R.S</a> .....  | 41        |
| 4.7      | <a href="#">UART</a> .....   | 42        |
| 4.8      | <a href="#">Fast I2C</a> .....   | 43        |
| 4.9      | <a href="#">Dual Staged Watchdog Timer</a> .....                           | 44        |
| 4.10     | <a href="#">Intel® Fast Flash Standby™ / Rapid Start Technology™</a> ..... | 45        |
| 4.11     | <a href="#">Speedstep Technology</a> .....                                 | 47        |
| 4.12     | <a href="#">C-States</a> .....   | 48        |
| 4.13     | <a href="#">Hyper Threading</a> .....                                      | 49        |
| 4.14     | <a href="#">Dynamic FSB Frequency Switching</a> .....                      | 50        |
| 4.15     | <a href="#">VID-x</a> .....  | 51        |
| 4.16     | <a href="#">Intel® Turbo Boost Technology and AVX</a> .....                | 52        |
| 4.17     | <a href="#">Display Configuration</a> .....                                | 53        |
| 4.18     | <a href="#">Hybrid Graphics / Multi-monitor</a> .....                      | 56        |
| 4.19     | <a href="#">Intel® Wireless Display</a> .....                              | 57        |
| 4.20     | <a href="#">Intel® vPro™ technology</a> .....                              | 59        |
| 4.21     | <a href="#">ACPI Suspend Modes and Resume Events</a> .....                 | 60        |
| <b>5</b> | <b><a href="#">System Resources</a>.....</b>                               | <b>61</b> |
| 5.1      | <a href="#">Interrupt Request (IRQ) Lines</a> .....                        | 61        |
| 5.2      | <a href="#">Memory Area</a> .....  | 62        |
| 5.3      | <a href="#">I/O Address Map</a> .....                                      | 62        |
| 5.4      | <a href="#">Peripheral Component Interconnect (PCI) Devices</a> .....      | 63        |
| 5.5      | <a href="#">Internal I2C Bus</a> .....                                     | 63        |
| 5.6      | <a href="#">External I2C Bus</a> .....                                     | 63        |
| 5.7      | <a href="#">System Management (SM) Bus</a> .....                           | 64        |
| <b>6</b> | <b><a href="#">Connectors</a>.....</b>                                     | <b>65</b> |
| 6.1      | <a href="#">Connector Location</a> .....                                   | 65        |
| <b>7</b> | <b><a href="#">Pinout List</a>.....</b>                                    | <b>66</b> |
| 7.1      | <a href="#">General Signal Description</a> .....                           | 66        |
| 7.2      | <a href="#">Connector X1A Row A</a> .....                                  | 67        |
| 7.3      | <a href="#">Connector X1A Row B</a> .....                                  | 69        |
| 7.4      | <a href="#">Connector X1B Row C</a> .....                                  | 71        |
| 7.5      | <a href="#">Connector X1B Row D</a> .....                                  | 73        |
| <b>8</b> | <b><a href="#">BIOS Operation</a>.....</b>                                 | <b>75</b> |
| 8.1      | <a href="#">Determining the BIOS Version</a> .....                         | 75        |
| 8.2      | <a href="#">BIOS Update</a> .....  | 75        |
| 8.3      | <a href="#">POST Codes</a> .....   | 75        |

|       |                                   |     |
|-------|-----------------------------------|-----|
| 8.4   | <a href="#">Setup Guide</a> ..... | 75  |
| 8.5   | <a href="#">BIOS Setup</a> .....  | 76  |
| 8.5.1 | <a href="#">Main</a> .....        | 76  |
| 8.5.2 | <a href="#">Advanced</a> .....    | 83  |
| 8.5.3 | <a href="#">Security</a> .....    | 125 |
| 8.5.4 | <a href="#">Boot</a> .....        | 127 |
| 8.5.5 | <a href="#">Exit</a> .....        | 128 |

# 1 User Information

## 1.1 Revision History

| Version | Brief Description of Change  | Date of Issue |
|---------|--|---------------|
| 1.10    | Initial version  |               |
| 2.0     | Removed ADA-LVDS-DVI 18-bit and 24-bit accessories<br>Updates SM bus 8-bit address information for the hardware monitor<br>Included a Revision History table | 2017-Aug-10   |
| 2.1     | Updates SPI Flash manufacturer information   | 2019-April-12 |
| 2.2     | Updates carrier board accessories  | 2020-Jul-23   |

## 1.2 About This Document

This document provides information about products from Kontron S&T AG and/or its subsidiaries also known as Kontron within this user guide. No warranty of suitability, purpose, or fitness is implied. While every attempt has been made to ensure that the information in this document is accurate, the information contained within is supplied “as-is” and is subject to change without notice.

For the circuits, descriptions and tables indicated, Kontron assumes no responsibility as far as patents or other rights of third parties are concerned.

## 1.3 Copyright Notice

Copyright © 2003-2018 Kontron S&T AG

All rights reserved. No part of this document may be reproduced, transmitted, transcribed, stored in a retrieval system, or translated into any language or computer language, in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise), without the express written permission of Kontron.

DIMM-PC®, PISA®, ETX®, ETXexpress®, microETXexpress®, X-board®, DIMM-IO® and DIMM-BUS® are trademarks or registered trademarks of Kontron. Kontron is trademark or registered trademark of Kontron S&T AG.

## 1.4 Trademarks

The following lists the trademarks of components used in this board.

- » IBM, XT, AT, PS/2 and Personal System/2 are trademarks of International Business Machines Corp.
- » Microsoft is a registered trademark of Microsoft Corp.
- » Intel is a registered trademark of Intel Corp.
- » All other products and trademarks mentioned in this manual are trademarks of their respective owners.

## 1.5 Standards

Kontron is ISO certified.

## 1.6 Warranty

For this Kontron product warranty for defects in material and workmanship exists as long as the warranty period, beginning with the date of shipment, lasts. During the warranty period, Kontron will decide on its discretion if defective products are to be repaired or replaced.

Within the warranty period, the repair of products is free of charge as long as warranty conditions are observed.

Warranty does not apply for defects arising/resulting from improper or inadequate maintenance or handling by the buyer, unauthorized modification or misuse, as well as the operation outside of the product's environmental specifications and improper installation and maintenance.

Kontron will not be responsible for any defects or damages to other products not supplied by Kontron that are caused by a faulty Kontron product.

## 1.7 Technical Support

Technicians and engineers from Kontron and/or its subsidiaries are available for technical support. We are committed to make our product easy to use and will help you use our products in your systems.

Please consult our Website at <http://www.kontron.com/support> for the latest product documentation, utilities, drivers and support contacts. Consult our customer section <http://emdcustomersection.kontron.com> for the latest BIOS downloads, Product Change Notifications, Board Support Packages, DemoImages, 3D drawings and additional tools and software. In any case you can always contact your board supplier for technical support.

## 2 Introduction

### 2.1 Product Description

The brand new application-ready COMe-bHL6 offers increased performance density and up to twice the graphics performance compared to its predecessors. Up to three independent, daisy-chained displays with up to 4K resolution are supported to create stunning user experiences. Further to this, DirectX® 11.1 and OpenGL 4.0 support paves the way for compelling visuals when videos, graphics and interactive content are being displayed. By integrating the new Intel® AVX2 and OpenCL 1.2, Kontron's new Computer-on-Modules additionally not only provide an increase in floating-point performance they also possess improved parallel processing capacities. Typical application areas can be found in markets such as digital signage, professional gaming and entertainment, medical imaging and surveillance and security as well as industrial plant and machine line control on shop floor- and control room-level.

Engineers can immediately commence with evaluating these new benchmark Computer-on-Modules on all Kontron COM Express® pin-out type 6-compliant starter kits.

The Kontron COM Express® pin-out type 6 COMe-bHL6 module is available in several different variants ranging from the cost-optimized low-power processor versions up to quad-core Intel® Core™ i7 processors with up to 4x 2.4 GHz. The modules are designed with the Intel® Mobile QM87 chipset, host up to 16 GB DDR3L RAM and support 7 PCI Express x1 lanes and 1 PEG x16 interface which is also compatible to standard PCI Express devices. Less complex peripherals can be connected via SPI and LPC. Additional dedicated features include 3x SATA 6Gb/s ports, 1 SATA 3Gb/s port, as well as Gigabit Ethernet, 4 USB 3.0 ports, 4 USB 2.0 and 2 serial ports. The Kontron COMe-bHL6 features comprehensive display support with 3x dual mode DisplayPort++ which can also output, HDMI, DVI and DisplayPort 1.2. Industrial applications benefit from the watchdog and real-time clock. The module supports an 8.5-20V wide-range power supply. The support of smart batteries via MARS and the standardized embedded application programming interface EAPI round off the feature set and provide engineers with a comprehensive service package that eases system development as well as system programming.

For customers wanting to instantly leverage the new graphics and computing power in their existing designs based on individual carrier boards, Kontron also offers standardized migration support services to accelerate the design-in phase and thus achieve fastest field deployment.

The Kontron COM Express® basic Computer-on-Module COMe-bHL6 supports the full Windows OS portfolio along with Linux and VxWorks.

### 2.2 Naming clarification

COM Express® defines a Computer-On-Module, or COM, with all components necessary for a bootable host computer, packaged as a super component.

- » COMe-bXX# modules are Kontron's COM Express® modules in basic form factor (125mm x 95mm)
- » COMe-cXX# modules are Kontron's COM Express® modules in compact form factor (95mm x 95mm)
- » COMe-mXX# modules are Kontron's COM Express® modules in mini form factor (55mm x 84mm)

The product names for Kontron COM Express® Computer-on-Modules consist of a short form of the industry standard (**COMe-**), the form factor (**b**=basic, **c**=compact, **m**=mini), the capital letters for the CPU and Chipset Codenames (**XX**) and the pin-out type (**#**) followed by the CPU Name.



## 2.3 Understanding COM Express® Functionality

All Kontron COM Express® basic and compact modules contain two 220pin connectors; each of it has two rows called Row A & B on primary connector and Row C & D on secondary connector. COM Express® Computer-on-modules feature the following maximum amount of interfaces according to the PICMG module Pin-out type:

| Feature                 | Pin-Out Type 1 | Pin-Out Type 10 | Pin-Out Type 2     | Pin-Out Type 6 |
|-------------------------|----------------|-----------------|--------------------|----------------|
| HD Audio                | 1x             | 1x              | 1x                 | 1x             |
| Gbit Ethernet           | 1x             | 1x              | 1x                 | 1x             |
| Serial ATA              | 4x             | 4x              | 4x                 | 4x             |
| Parallel ATA            | -              | -               | 1x                 | -              |
| PCI                     | -              | -               | 1x                 | -              |
| PCI Express x1          | 6x             | 6x              | 6x                 | 8x             |
| PCI Express x16 (PEG)   | -              | -               | 1x                 | 1x             |
| USB Client              | 1x             | 1x              | -                  | -              |
| USB 2.0                 | 8x             | 8x              | 8x                 | 8x             |
| USB 3.0                 | -              | 2x              | -                  | 4x             |
| VGA                     | 1x             | -               | 1x                 | 1x             |
| LVDS                    | Dual Channel   | Single Channel  | Dual Channel       | Dual Channel   |
| DP++ (SDVO/DP/HDMI/DVI) | 1x optional    | 1x              | 3x shared with PEG | 3x             |
| LPC                     | 1x             | 1x              | 1x                 | 1x             |
| External SMB            | 1x             | 1x              | 1x                 | 1x             |
| External I2C            | 1x             | 1x              | 1x                 | 1x             |
| GPIO                    | 8x             | 8x              | 8x                 | 8x             |
| SDIO shared w/GPIO      | 1x optional    | 1x optional     | -                  | 1x optional    |
| UART (2-wire COM)       | -              | 2x              | -                  | 2x             |
| FAN PWM out             | -              | 1x              | -                  | 1x             |

## 2.4 COM Express® Documentation

This product manual serves as one of three principal references for a COM Express® design. It documents the specifications and features of COMe-bHL6. Additional references are available at your Kontron Support or at PICMG®:

- » The COM Express® Specification defines the COM Express® module form factor, pin-out, and signals. This document is available at the PICMG® website by filling out the order form.
- » The COM Express® Design Guide by PICMG® serves as a general guide for baseboard design, with a focus on maximum flexibility to accommodate a wide range of COM Express® modules.



Some of the information contained within this product manual applies only to certain product revisions (CE: xxx). If certain information applies to specific product revisions (CE: xxx) it will be stated. Please check the product revision of your module to see if this information is applicable.

## 2.5 COM Express® Benefits

COM Express® modules are very compact, highly integrated computers. All Kontron COM Express® modules feature a standardized form factor and a standardized connector layout which carry a specified set of signals. Each COM is based on the COM Express® specification. This standardization allows designers to create a single-system baseboard that can accept present and future COM Express® modules.

The baseboard designer can optimize exactly how each of these functions implements physically. Designers can place connectors precisely where needed for the application on a baseboard designed to optimally fit a system's packaging.

A single baseboard design can use a range of COM Express® modules with different sizes and pin-outs. This flexibility can differentiate products at various price/performance points, or when designing future proof systems that have a built-in upgrade path. The modularity of a COM Express® solution also ensures against obsolescence when computer technology evolves. A properly designed COM Express® baseboard can work with several successive generations of COM Express® modules.

A COM Express® baseboard design has many advantages of a customized computer-board design and, additionally, delivers better obsolescence protection, heavily reduced engineering effort, and faster time to market.

## 3 Product Specification

### 3.1 Module definition

The COM Express® basic sized Computer-on-Module COMe-bHL6 (BHL6 / BBL6) follows pin-out Type 6 and is compatible to PICMG specification COM.0 Rev 2.1. The COMe-bHL6 based on latest Shark Bay Mobile platform is available in different variants to cover the demand of different performance, price and power:

#### Commercial grade modules (0°C to 60°C operating)

| Product Number  | Product Name        | Processor              | TDP     | PCH  | USB 3.0 | SATA 6G | SATA 3G |
|-----------------|---------------------|------------------------|---------|------|---------|---------|---------|
| 38025-0000-18-7 | COMe-bHL6 i7-4860EQ | Intel® Core™ i7-4860EQ | 47W     | QM87 | 4       | 3       | 1       |
| 38025-0000-16-7 | COMe-bHL6 i7-4850EQ | Intel® Core™ i7-4850EQ | 47W     | QM87 | 4       | 3       | 1       |
| 38025-0000-24-7 | COMe-bHL6 i7-4700EQ | Intel® Core™ i7-4700EQ | 47W/37W | QM87 | 4       | 3       | 1       |
| 38025-0000-29-5 | COMe-bHL6 i5-4410E  | Intel® Core™ i5-4410E  | 37W     | QM87 | 4       | 3       | 1       |
| 38025-0000-27-5 | COMe-bHL6 i5-4400E  | Intel® Core™ i5-4400E  | 37W     | QM87 | 4       | 3       | 1       |
| 38025-0000-18-5 | COMe-bHL6 i5-4422E  | Intel® Core™ i5-4422E  | 25W     | QM87 | 4       | 3       | 1       |
| 38025-0000-16-5 | COMe-bHL6 i5-4402E  | Intel® Core™ i5-4402E  | 25W     | QM87 | 4       | 3       | 1       |
| 38025-0000-26-3 | COMe-bHL6 i3-4110E  | Intel® Core™ i3-4110E  | 37W     | HM86 | 2       | 2       | 2       |
| 38025-0000-24-3 | COMe-bHL6 i3-4100E  | Intel® Core™ i3-4100E  | 37W     | HM86 | 2       | 2       | 2       |
| 38025-0000-18-3 | COMe-bHL6 i3-4112E  | Intel® Core™ i3-4112E  | 25W     | HM86 | 2       | 2       | 2       |
| 38025-0000-16-3 | COMe-bHL6 i3-4102E  | Intel® Core™ i3-4102E  | 25W     | HM86 | 2       | 2       | 2       |
| 38025-0000-22-1 | COMe-bHL6 2000E     | Intel® Celeron 2000E   | 37W     | HM86 | 2       | 2       | 2       |
| 38025-0000-15-1 | COMe-bHL6 2002E     | Intel® Celeron 2002E   | 25W     | HM86 | 2       | 2       | 2       |

#### Extended temperature grade modules (E1, -25°C to 75°C operating) and

#### Industrial temperature grade modules (XT, -40°C to 85°C operating)

The COMe-bHL6 is available for extended and industrial temperature range. General capability was tested for following options:

- » CPU: all
- » Memory: E2 DDR3L memory only 97015-xxxx-16-3
- » VCC: 12V only, no support for Wide-Range Input

The RXT product line includes modules with following featureset:

- » industrial grade temperature range (-40 to +85°C) by screening
- » ECC Memory support (97016-xxxx-16-3)
- » Kontron Rapid Shutdown support

| Product Number  | Product Name           | Processor              | TDP     | PCH  | USB 3.0 | SATA 6G | SATA 3G |
|-----------------|------------------------|------------------------|---------|------|---------|---------|---------|
| 38026-0000-18-7 | COMe-bHL6RXT i7-4860EQ | Intel® Core™ i7-4860EQ | 47W     | QM87 | 4       | 3       | 1       |
| 38026-0000-24-7 | COMe-bHL6RXT i7-4700EQ | Intel® Core™ i7-4700EQ | 47W/37W | QM87 | 4       | 3       | 1       |
| 38026-0000-29-5 | COMe-bHL6RXT i5-4410E  | Intel® Core™ i5-4410E  | 37W     | QM87 | 4       | 3       | 1       |
| 38026-0000-27-5 | COMe-bHL6RXT i5-4400E  | Intel® Core™ i5-4400E  | 37W     | QM87 | 4       | 3       | 1       |
| 38026-0000-18-5 | COMe-bHL6RXT i5-4422E  | Intel® Core™ i5-4422E  | 25W     | QM87 | 4       | 3       | 1       |



Please contact your local sales for further information and MOQ for RXT modules

## 3.2 Functional Specification

### Processor

The 22nm Intel® 4th Gen Core™ i7/i5/i3/Celeron® embedded (Haswell-H (Halo) / Crystal Well) CPU family with 37.5x32mm package size (BGA1364 socket) supports:

- » Intel® Turbo Boost Technology 2.01
- » Intel® 64
- » Intel® Virtualization Technology (VT-x)
- » Intel® Virtualization Technology for Directed I/O (VT-d)
- » Intel® Hyper-Threading Technology
- » Enhanced Intel SpeedStep® Technology
- » Idle States (C-States)
- » Intel® Smart Cache
- » Thermal Monitoring Technologies
- » Intel® Fast Memory Access
- » Intel® Flex Memory Access
- » Integrated Intel® HD Graphics with Dynamic Frequency

Optional available (with customized BIOS, Evaluation Copy on request):

- » Intel® vPRO™ Technology including:
  - » Intel® Active Management Technology (AMT)
  - » Intel® Trusted Execution Technology (TXT)
  - » Advanced Encryption Standard Instructions (AES-NI)

The integrated Intel® HD Graphics 5200/4600 supports:

- » GraphicsTechnology GT3 with 40 Execution Units (HD5200)
- » GraphicsTechnology GT2 with 20 Execution Units (HD4600)
- » Intel® Quick Sync Video
- » Intel® InTru™ 3D Technology
- » Intel® Wireless Display
- » Intel® Flexible Display Interface (Intel® FDI)
- » Intel® Clear Video HD Technology
- » Intel® Graphics Render C-State RC6
- » Intel® Smart 2D Display Technology (S2DDT)
- » 3 simultaneous displays (Win7/8 and Linux)
- » Hybrid Multi Monitor with 2 internal and 2 external displays
- » Video Decode for AVC/H.264/VC-1/MPEG-2
- » Video Encode for AVC/H.264/MPEG-2
- » Blu-ray Playback (incl. PAVP)

The integrated Intel® HD Graphics supports:

- » GraphicsTechnology GT1 with 10 Execution Units
- » Dual Display
- » Video Decode for AVC/H.264/VC-1/MPEG-2
- » Video Encode for AVC/H.264/MPEG-2
- » Blu-ray Playback (incl. PAVP)

## CPU Features

| Intel®                         | Core™           | Core™           | Core™          | Core™          | Core™          | Core™          | Core™          | Celeron®       | Celeron®       |
|--------------------------------|-----------------|-----------------|----------------|----------------|----------------|----------------|----------------|----------------|----------------|
| -                              | i7-4860EQ       | i7-4850EQ       | i7-4700EQ      | i5-4400E       | i5-4402E       | i3-4100E       | i3-4102E       | 2000E          | 2002E          |
| # of Cores                     | 4               | 4               | 4              | 2              | 2              | 2              | 2              | 2              | 2              |
| # of Threads                   | 8               | 8               | 8              | 4              | 4              | 4              | 4              | 2              | 2              |
| TDP Core frequency (HFM)       | <b>1800MHz</b>  | <b>1600MHz</b>  | <b>2400MHz</b> | <b>2700MHz</b> | <b>1600MHz</b> | <b>2400MHz</b> | <b>1600MHz</b> | <b>2200MHz</b> | <b>1500MHz</b> |
| Max Turbo Frequency 1 core     | 3200MHz         | 3200MHz         | 3400MHz        | 3300MHz        | 2700MHz        | -              | -              | -              | -              |
| Max Turbo all cores            | 2600MHz         | 2600MHz         | 2800MHz        | 3200MHz        | 2600MHz        | -              | -              | -              | -              |
| LFM/LPM Frequency              | 800MHz          | 800MHz          | 800MHz         | 800MHz         | 800MHz         | 800MHz         | 800MHz         | 800MHz         | 800MHz         |
| Bus/Core Ratio                 | 8 - 20          | 8 - 16          | 8 - 24         | 8 - 27         | 8 - 16         | 8 - 24         | 8 - 16         | 8 - 22         | 8 - 15         |
| TjMax                          | 100°C           | 100°C           | 100°C          | 100°C          | 100°C          | 100°C          | 100°C          | 100°C          | 100°C          |
| Thermal Design Power (TDP/PL1) | 47W             | 47W             | 47W            | 37W            | 25W            | 37W            | 25W            | 37W            | 25W            |
| cTDP-Down                      | -               | -               | 37W            | -              | -              | -              | -              | -              | -              |
| cTDP-Down Core frequency       | -               | -               | <b>1700MHz</b> | -              | -              | -              | -              | -              | -              |
| Power Limit 2 (PL2 max)        | 58.75W          | 58.75W          | 58.75/46.25 W  | 46.25W         | 31.25W         | 46.25W         | 31.25W         | 46.25W         | 31.25W         |
| C-States                       | C0-C7           | C0-C7           | C0-C7          | C0-C7          | C0-C7          | C0-C7          | C0-C7          | C0-C7          | C0-C7          |
| eDRAM                          | 128MB<br>1.6GHz | 128MB<br>1.6GHz | -              | -              | -              | -              | -              | -              | -              |
| Smart Cache                    | 6MB             | 6MB             | 6MB            | 3MB            | 3MB            | 3MB            | 3MB            | 2MB            | 2MB            |
| Min Memory Type                | DDR3L-1066      | DDR3L-1066      | DDR3L-1066     | DDR3L-1066     | DDR3L-1066     | DDR3L-1066     | DDR3L-1066     | DDR3L-1066     | DDR3L-1066     |
| Max Memory Type                | DDR3L-1600      | DDR3L-1600      | DDR3L-1600     | DDR3L-1600     | DDR3L-1600     | DDR3L-1600     | DDR3L-1600     | DDR3L-1600     | DDR3L-1600     |
| Max Memory Size                | 2x8GB           | 2x8GB           | 2x8GB          | 2x8GB          | 2x8GB          | 2x8GB          | 2x8GB          | 2x8GB          | 2x8GB          |
| # of Memory Channels           | 2               | 2               | 2              | 2              | 2              | 2              | 2              | 2              | 2              |
| Graphics Model                 | Iris Pro 5200   | Iris Pro 5200   | HD4600         | HD4600         | HD4600         | HD4600         | HD4600         | HD             | HD             |
| GFX LFM Frequency              | 200MHz          | 200MHz          | 200MHz         | 200MHz         | 200MHz         | 200MHz         | 200MHz         | 200MHz         | 200MHz         |
| GFX Base Frequency             | 650MHz          | 750MHz          | 400MHz         | 400MHz         | 400MHz         | 400MHz         | 400MHz         | 400MHz         | 400MHz         |
| GFX Turbo Frequency            | 1000MHz         | 1000MHz         | 1000MHz        | 1000MHz        | 900MHz         | 900MHz         | 900MHz         | 900MHz         | 900MHz         |
| GFX Technology                 | GT3e 40EU       | GT3e 40EU       | GT2 20EU       | GT2 20EU       | GT2 20EU       | GT2 20EU       | GT2 20EU       | GT1 10EU       | GT1 10EU       |
| GFX Func/Phys Cores            | 3/3             | 3/3             | 2/2            | 2/2            | 2/2            | 2/2            | 2/2            | 1/2            | 1/2            |
| Quick Sync Video               | Yes             | Yes             | Yes            | Yes            | Yes            | Yes            | Yes            | -              | -              |
| InTru™ 3D                      | Yes             | Yes             | Yes            | Yes            | Yes            | Yes            | Yes            | -              | -              |
| Wireless Display               | Yes             | Yes             | Yes            | Yes            | Yes            | Yes            | Yes            | -              | -              |
| Clear Video HD                 | Yes             | Yes             | Yes            | Yes            | Yes            | Yes            | Yes            | -              | -              |
| vPRO™ (optional)               | Yes             | Yes             | Yes            | Yes            | Yes            | -              | -              | -              | -              |
| TXT (optional)                 | Yes             | Yes             | Yes            | Yes            | Yes            | -              | -              | -              | -              |
| AES-NI (optional)              | Yes             | Yes             | Yes            | Yes            | Yes            | -              | -              | -              | -              |
| VT-x                           | Yes             | Yes             | Yes            | Yes            | Yes            | -              | -              | -              | -              |
| VT-d                           | Yes             | Yes             | Yes            | Yes            | Yes            | -              | -              | -              | -              |
| PCI Express Graphics x16       | Gen 3.0         | Gen 3.0         | Gen 3.0        | Gen 3.0        | Gen 3.0        | Gen 3.0        | Gen 3.0        | Gen 2.0        | Gen 2.0        |

| Intel®                         | Core™          | Core™          | Core™          | Core™          |
|--------------------------------|----------------|----------------|----------------|----------------|
| -                              | i5-4410E       | i5-4422E       | i3-4110E       | i3-4112E       |
| # of Cores                     | 2              | 2              | 2              | 2              |
| # of Threads                   | 4              | 4              | 4              | 4              |
| TDP Core frequency (HFM)       | <b>2900MHz</b> | <b>1800MHz</b> | <b>2600MHz</b> | <b>1800MHz</b> |
| Max Turbo Frequency 1 core     | Note 1         | 2900MHz        | -              | -              |
| Max Turbo all cores            | Note 1         | 2800MHz        | -              | -              |
| LFM/LPM Frequency              | 800MHz         | 800MHz         | 800MHz         | 800MHz         |
| Bus/Core Ratio                 | 8 - 29         | 8 - 16         | 8 - 24         | 8 - 16         |
| TjMax                          | 100°C          | 100°C          | 100°C          | 100°C          |
| Thermal Design Power (TDP/PL1) | 37W            | 25W            | 37W            | 25W            |
| cTDP-Down                      | -              | -              | -              | -              |
| cTDP-Down Core frequency       | -              | -              | -              | -              |
| Power Limit 2 (PL2 max)        | 46.25W         | 31.25W         | 46.25W         | 31.25W         |
| C-States                       | C0-C7          | C0-C7          | C0-C7          | C0-C7          |
| eDRAM                          | -              | -              | -              | -              |
| Smart Cache                    | 3MB            | 3MB            | 3MB            | 3MB            |
| Min Memory Type                | DDR3L-1066     | DDR3L-1066     | DDR3L-1066     | DDR3L-1066     |
| Max Memory Type                | DDR3L-1600     | DDR3L-1600     | DDR3L-1600     | DDR3L-1600     |
| Max Memory Size                | 2x8GB          | 2x8GB          | 2x8GB          | 2x8GB          |
| # of Memory Channels           | 2              | 2              | 2              | 2              |
| Graphics Model                 | HD4600         | HD4600         | HD4600         | HD4600         |
| GFX LFM Frequency              | 200MHz         | 200MHz         | 200MHz         | 200MHz         |
| GFX Base Frequency             | 400MHz         | 400MHz         | 400MHz         | 400MHz         |
| GFX Turbo Frequency            | 1000MHz        | 900MHz         | 900MHz         | 900MHz         |
| GFX Technology                 | GT2 20EU       | GT2 20EU       | GT2 20EU       | GT2 20EU       |
| GFX Func/Phys Cores            | 2/2            | 2/2            | 2/2            | 2/2            |
| Quick Sync Video               | Yes            | Yes            | Yes            | Yes            |
| InTru™ 3D                      | Yes            | Yes            | Yes            | Yes            |
| Wireless Display               | Yes            | Yes            | Yes            | Yes            |
| Clear Video HD                 | Yes            | Yes            | Yes            | Yes            |
| vPRO™ (optional)               | Yes            | Yes            | -              | -              |
| TXT (optional)                 | Yes            | Yes            | -              | -              |
| AES-NI (optional)              | Yes            | Yes            | Yes            | Yes            |
| VT-x                           | Yes            | Yes            | Yes            | Yes            |
| VT-d                           | Yes            | Yes            | -              | -              |
| PCI Express Graphics x16       | Gen 3.0        | Gen 3.0        | Gen 3.0        | Gen 3.0        |

## Memory

|              |                              |
|--------------|------------------------------|
| Sockets      | 2x DDR3 SO-DIMM              |
| Memory Type  | DDR3L-1600 (ECC on RXT Ver.) |
| Maximum Size | 2x8GB                        |
| Technology   | Dual Channel                 |

## Chipset

The 32nm Intel® 8-Series Platform Controller Hub Lynx Point supports:

- » PCI Express Revision 2.0
- » PCI Express Configurations x1, x2, x4
- » Intel® Virtualization Technology for Directed I/O (VT-d)
- » Intel® Trusted Execution Technology (TXT)
- » Intel® vPro Technology (optional)
- » Intel® Active Management Technology 9.0 (optional)
- » Intel® Anti-Theft Technology
- » Intel® Rapid Storage Technology
- » Intel® Smart Response Technology

## PCH comparison

| Feature                      | QM87                 | HM86             |
|------------------------------|----------------------|------------------|
| TDP                          | 2.7W                 | 2.7W             |
| USB 3.0 (USB 2.0 compatible) | YES (4x on COMe)     | YES (2x on COMe) |
| USB 2.0                      | YES (4x on COMe)     | YES (6x on COMe) |
| SATA 6Gb/s (Gen3)            | YES (3x on COMe)     | YES (2x on COMe) |
| SATA 3Gb/s (Gen2)            | YES (1x on COMe)     | YES (2x on COMe) |
| Wireless Display             | YES                  | YES              |
| 3 Displays simultaneously    | YES                  | YES              |
| Rapid Storage                | AHCI, RAID 0/1/5/10  | AHCI only        |
| VT-d                         | YES                  | NO               |
| vPRO                         | YES with custom BIOS | NO               |
| AMT                          | YES with custom BIOS | NO               |
| TXT                          | YES with custom BIOS | NO               |



The Intel® vPro Technology including Trusted Execution Technology (TXT), Active Management Technology (AMT) and Encryption AES-NI is not supported by default on COMe-bHL6. Please contact your local sales or support for custom BIOS variants supporting vPro.



## HighSpeed I/O Port Configuration

|        | QM87 I/O            | HM86 I/O           | COMe-bHL6 with QM87  | COMe-bHL6 with HM86  |
|--------|---------------------|--------------------|----------------------|----------------------|
| -      | USB3 #1             | USB3 #1            | USB #0 = USB3.0      | USB #0 = USB3.0      |
| Port1  | USB3 #1             | USB3 #1            | USB #0 = USB3.0      | USB #0 = USB3.0      |
| Port2  | USB3 #2             | USB3 #2            | USB #1 = USB3.0      | USB #1 = USB3.0      |
| Port3  | USB3 #5             | -                  | USB #2 = USB3.0      | -                    |
| Port4  | USB3 #6             | -                  | USB #3 = USB3.0      | -                    |
| -      | USB2                | USB2               | USB #4-7 = USB 2.0   | USB #2-7 = USB 2.0   |
| Port5  | USB3 #3 or PCIe #1  | USB3 #3 or PCIe #1 | PCIe #0              | PCIe #0              |
| Port6  | USB3 #4 or PCIe #2  | USB3 #4 or PCIe #2 | PCIe #1              | PCIe #1              |
| Port7  | PCIe #3             | PCIe #3            | PCIe #2              | PCIe #2              |
| Port8  | PCIe #4             | PCIe #4            | PCIe #3              | PCIe #3              |
| Port9  | PCIe #5             | PCIe #5            | PCIe #4              | PCIe #4              |
| Port10 | PCIe #6             | PCIe #6            | PCIe #5              | PCIe #5              |
| Port11 | PCIe #7             | PCIe #7            | PCIe #6              | PCIe #6              |
| Port12 | PCIe #8             | PCIe #8            | LAN/PCIe #7          | LAN/PCIe #7          |
| Port13 | SATA3 #4 or PCIe #1 | SATA3 #4           | SATA #0 = SATA 6Gb/s | SATA #0 = SATA 6Gb/s |
| Port14 | SATA3 #5 or PCIe #2 | SATA3 #5           | SATA #1 = SATA 6Gb/s | SATA #1 = SATA 6Gb/s |
| Port15 | SATA3 #0            | SATA2 #0           | SATA #2 = SATA 6Gb/s | SATA #2 = SATA 3Gb/s |
| Port16 | SATA3 #1            | -                  | -                    | -                    |
| Port17 | SATA2 #2            | SATA2 #2           | SATA #3 = SATA 3Gb/s | SATA #3 = SATA 3Gb/s |
| Port18 | SATA2 #3            | -                  | -                    | -                    |

## Graphics Core

The integrated Intel® HD/HD4600/HD5200 (Gen7.5) supports:

|                                   |  |
|-----------------------------------|--|
| Graphics Core Render Clock        | GT1/GT2/GT3; Base clock: 400/200 MHz; GT Turbo: up to 1000 MHz |
| Execution Units / Pixel Pipelines | GT3: 40EU / GT2: 20EU / GT1: 10EU                              |
| Max Graphics Memory               | 1720MB   |
| GFX Memory Bandwidth (GB/s)       | 25.6   |
| GFX Memory Technology             | DVMT   |
| API (DirectX/OpenGL)              | 11.1 / 4.0 + OCL 1.2   |
| Shader Model                      | 5.0  |
| Hardware accelerated Video        | MPEG2, VC-1, AVC, Blu-ray (+3D)                                |
| Independent/Simultaneous Displays | 3  |
| Display Port                      | DP 1.2 / eDP 1.3   |
| HDCP support                      | HDCP 1.4a  |

## Monitor output

|                    |           |
|--------------------|-----------|
| CRT max Resolution | 1920x1200 |
| TV out:            | -         |

## LVDS

|                                |                               |
|--------------------------------|-------------------------------|
| LVDS Bits/Pixel                | 1x18/24, 2x18/24 with DP2LVDS |
| LVDS Bits/Pixel with dithering | -                             |
| LVDS max Resolution:           | 1920x1200                     |
| PWM Backlight Control:         | YES                           |
| Supported Panel Data:          | JILI2/JILI3/EDID/DID          |

## Display Interfaces

|                                |                                |
|--------------------------------|--------------------------------|
| Discrete Graphics              | 1x PEG 3.0/2.0                 |
| Digital Display Interface DDI1 | DP++                           |
| Digital Display Interface DDI2 | DP++                           |
| Digital Display Interface DDI3 | DP++                           |
| Maximum Resolution on DDI      | HDMI: 4096x2304, DP: 3840x2160 |

## PEG Configuration

The x16 PCI Express Graphics Port (PEG) is compatible to standard PCI Express devices like Ethernet or RAID controllers. The COMe-bHL6 supports following PEG Port configuration when used as PCI Express Interface:

- » 1×16
- » 1×8
- » 1×4
- » 1×2
- » 1×1

The internal PCI Express controller can be re-configured to support up to 3 PCIe ports on PEG16 interface. The PEG lane splitting is configurable in setup:

- » 1×16 (lanes #0-15)
- » 2×8 (lanes #0-7 + #8-15)
- » 1×8 + 2×4 (lanes #0-7 + #8-11 + #12-15)



With splitted ports, Port2 (#8-15 or #8-11) and Port3 (#12-15) cannot have more lanes active as Port1 (#0-7) has

## Storage

|                 |   |
|-----------------|---|
| onboard SSD     | -   |
| SD Card support | -   |
| IDE Interface   | -   |
| Serial-ATA      | up to 3x SATA 6Gb/s, 1x SATA 3Gb/s                    |
| SATA AHCI       | NCQ, HotPlug, Staggered Spinup, eSATA, PortMultiplier |
| SATA RAID       | 0, 1, 5, 10 (QM87 only)                               |



If SATA AHCI or RAID is disabled in setup, the SATA Interface only supports 3Gb/s transfer rate and Staggered Spin-Up. To configure a RAID Setup connect at least two hard drives and enable RAID support in BIOS Advanced/HDD Settings. After reboot, setup your RAID configuration in the new setup item "Addon Devices"

## Connectivity

|                                 |                             |
|---------------------------------|-----------------------------|
| USB 2.0                         | 8x USB 2.0                  |
| USB 3.0                         | up to 4x USB 3.0            |
| USB Client                      | -                           |
| PCI                             | -                           |
| PCI External Masters            | -                           |
| PCI Express                     | 7x PCIe x1 Gen 2.0          |
| Max PCI Express                 | 8x PCIe without LAN         |
| PCI Express x2/x4 configuration | YES (Softstrap option)      |
| Ethernet                        | 10/100/1000 Mbit            |
| Ethernet controller             | Intel® i218-LM (Clarkville) |

## PCI Express Configuration

By default, the COMe-bHL6 supports x1 PCIexpress lane configuration only (Configuration 0). Following x2/x4 configurations are available via Management Engine Softstrap Options with a customized Flash Descriptor.

| PCIe            | Port #0 | Port #1 | Port #2 | Port #3 | Port #4 | Port #5 | Port #6 | Port #7* |
|-----------------|---------|---------|---------|---------|---------|---------|---------|----------|
| Configuration 0 | x1      | x1      | x1      | x1      | x1      | x1      | x1      | x1       |
| Configuration 1 | x2      |         | x1      | x1      | x1      | x1      | x1      | x1       |
| Configuration 2 | x2      |         | x2      |         | x1      | x1      | x1      | x1       |
| Configuration 3 | x2      |         | x2      |         |         | x2      | x1      | x1       |
| Configuration 4 | x2      |         | x2      |         |         | x2      |         | x2       |
| Configuration 5 |         |         | x4      |         | x1      | x1      | x1      | x1       |
| Configuration 6 |         |         | x4      |         |         | x2      | x1      | x1       |
| Configuration 7 |         |         | x4      |         |         | x2      |         | x2       |
| Configuration 8 |         |         | x4      |         |         |         | x4      |          |



- \*PCIe Port #7 is available without Ethernet Controller only
- Configuration 0 is the default setting
- Configuration 3 & Configuration 5 are available in UEFI download package on EMD Customer Section

## Ethernet

The Intel® i218-LM (Clarkville) ethernet supports:

- » Jumbo Frames - 9K
- » MACsec IEEE 802.1 AE
- » Time Sync Protocol Indicator
- » WOL (Wake On LAN)
- » PXE (Preboot eXecution Environment)
- » IEEE1588

## Misc Interfaces and Features

|                          |                                    |
|--------------------------|------------------------------------|
| Supported BIOS Size/Type | 16MB SPI                           |
| Audio                    | HD Audio + DisplayPort dual stream |
| Onboard Hardware Monitor | Nuvoton NCT7802Y                   |
| Trusted Platform Module  | Atmel AT97SC3204-U2A1A-10          |
| Miscellaneous            | 2x UART / PWM FAN / eDP optional   |

## Kontron Features

|                                     |                               |
|-------------------------------------|-------------------------------|
| External I2C Bus                    | Fast I2C, MultiMaster capable |
| Smart Battery (M.A.R.S.) support    | YES                           |
| Embedded API                        | KEAPI3                        |
| Custom BIOS Settings / Flash Backup | YES                           |
| Watchdog support                    | Dual Staged                   |

## Additional features

- » All solid capacitors (POSCAP). No tantalum capacitors used.
- » Optimized RTC Battery monitoring to secure highest longevity
- » Real fast I2C with transfer rates up to 40kB/s.
- » Discharge logic on all onboard voltages for highest reliability

## Power Features

|                       |                  |
|-----------------------|------------------|
| Singly Supply Support | YES              |
| Supply Voltage        | 8.5V - 20V       |
| ACPI                  | ACPI 4.0         |
| S-States              | S0, S3, S4, S5   |
| S5 Eco Mode           | YES              |
| Misc Power Management | cTDP @ i7-4700EQ |

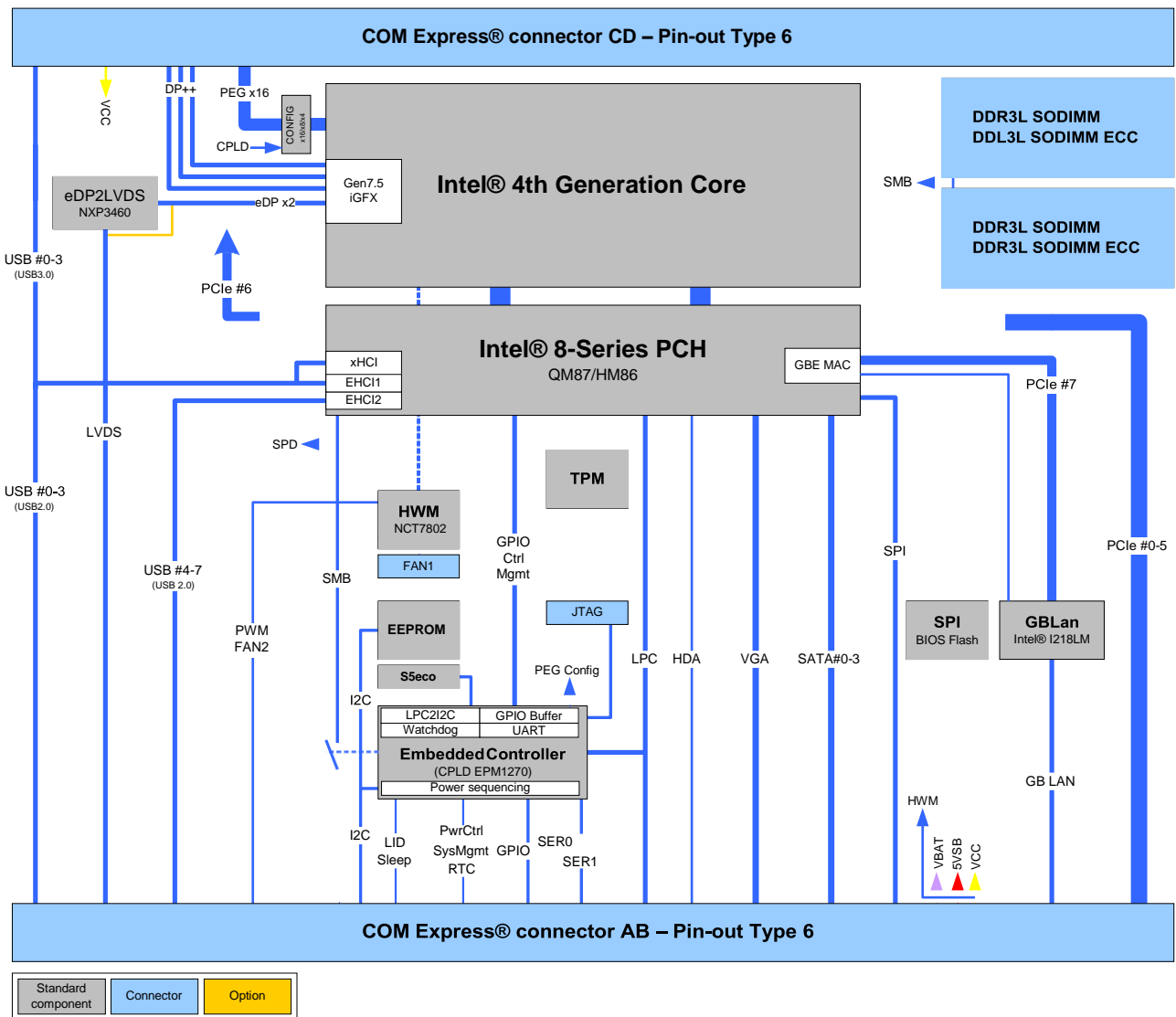
## Power Consumption and Performance

|                             |                |
|-----------------------------|----------------|
| Full Load Power Consumption | 17 - 48W       |
| Kontron Performance Index   | 32645 - 100815 |
| Kontron Performance/Watt    | 1723 - 3105    |



Detailed Power Consumption measurements and benchmarks for CPU, Graphics and Memory are available in Application Note [KEMAP054](#) at [EMD Customer Section](#).

### 3.3 Block Diagram



## 3.4 Accessories

### Product specific accessories

| Product Number     | Heatspreader and Cooling Solutions | Comment   |
|--------------------|------------------------------------|---|
| 38025-0000-99-2    | HSP COMe-bHL6 heatpipe thread      | For all CPUs and temperature grades                 |
| 38025-0000-99-3    | HSP COMe-bHL6 heatpipe through     | For all CPUs and temperature grades                 |
| 38025-0000-99-0C05 | HSK COMe-bHL6 active (w/o HSP)     | For all CPUs and commercial temperature grade usage |
| 38025-0000-99-0C06 | HSK COMe-bHL6 passive (w/o HSP)    | For all CPUs and commercial temperature grade usage |

### General accessories

| Part Number     | COMe pin-out Type 6 compatible accessories | Project Code  | Comment                                       |
|-----------------|--|---|---|
| 38116-0000-00-5 | COM Express® Eval Carrier2 Type 6          | ADT6  | ATX Carrier with 5mm COMe connector           |
| 96007-0000-00-3 | ADA-PCIe-DP                                | APDP  | PCIe x16 to DP Adapter for Evaluation Carrier |
| 96007-0000-00-7 | ADA-Type6-DP3                              | DVO6  | (sandwich) Adapter Card for 3x DisplayPort    |
| 96006-0000-00-2 | COMe POST T6                               | NFCB  | POST Code / Debug Card                        |
| 38019-0000-00-0 | ADA-COMe-Height-dual                       | EERC  | Height Adapter                                |
| Part Number     | Mounting                                   | Comment   |   |
| 38017-0000-00-5 | COMe Mount KIT 5mm 1set                    | Mounting Kit for 1 module including screws for 5mm connectors           |   |
| 38017-0100-00-5 | COMe Mount KIT 5mm 100sets                 | Mounting Kit for 100 modules including screws for 5mm connectors        |   |
| 38017-0000-00-0 | COMe Mount KIT 8mm 1set                    | Mounting Kit for 1 module including screws for 8mm connectors           |   |
| 38017-0100-00-0 | COMe Mount Kit 8mm 100sets                 | Mounting Kit for 100 modules including screws for 8mm connectors        |   |
| Part Number     | Cooling Solutions                          | Comment   |   |
| 36099-0000-99-0 | COMe Active Uni Cooler                     | for CPUs up to 20W TDP, to be mounted on HSP                            |   |
| 36099-0000-99-1 | COMe Passive Uni Cooler                    | for CPUs up to 10W TDP, to be mounted on HSP                            |   |
| Part Number     | Display Adapter                            | Comment   |   |
| 96006-0000-00-8 | ADA-DP-LVDS                                | DP to LVDS adapter  |   |
| 96082-0000-00-0 | KAB-ADAPT-DP-DVI                           | DP to DVI adapter cable   |   |
| 96083-0000-00-0 | KAB-ADAPT-DP-VGA                           | DP to VGA adapter cable   |   |
| 96084-0000-00-0 | KAB-ADAPT-DP-HDMI                          | DP to HDMI adapter cable  |   |
| Part Number     | Cables                                     | Comment   |   |
| 96079-0000-00-0 | KAB-HSP 200mm                              | Cable adapter to connect FAN to module (COMe basic/compact)             |   |
| 96079-0000-00-2 | KAB-HSP 40mm                               | Cable adapter to connect FAN to module (COMe basic/compact)             |   |
| Part Number     | Miscellaneous                              | Comment   |   |
| 18029-0000-00-0 | MARS Smart Battery Kit                     | Starterkit Kontron Mobile Application platform for Rechargeable Systems |   |

### For COMe-bHL6 standard (38025-xxxx-xx-x)

| Part Number     | DDR3L SODIMM, commercial temperature grade |
|-----------------|--|
| 97015-1024-16-1 | DDR3L-1600 SODIMM 1GB                      |
| 97015-2048-16-1 | DDR3L-1600 SODIMM 2GB                      |
| 97015-4096-16-1 | DDR3L-1600 SODIMM 4GB                      |
| 97015-8192-16-1 | DDR3L-1600 SODIMM 8GB                      |
| Part Number     | DDR3L SODIMM, industrial temperature grade |
| 97015-1024-16-3 | DDR3L-1600 SODIMM 1GB E2                   |
| 97015-2048-16-3 | DDR3L-1600 SODIMM 2GB E2                   |
| 97015-4096-16-3 | DDR3L-1600 SODIMM 4GB E2                   |
| 97015-8192-16-3 | DDR3L-1600 SODIMM 8GB E2                   |

### For COMe-bHL6RXT (38026-xxxx-xx-x)

| Part Number     | DDR3L ECC SODIMM, industrial temperature grade |
|-----------------|--|
| 97016-1024-16-3 | DDR3L-1600 SODIMM 1GB ECC E2                   |
| 97016-2048-16-3 | DDR3L-1600 SODIMM 2GB ECC E2                   |
| 97016-4096-16-3 | DDR3L-1600 SODIMM 4GB ECC E2                   |
| 97016-8192-16-3 | DDR3L-1600 SODIMM 8GB ECC E2                   |

## 3.5 Electrical Specification

### 3.5.1 Supply Voltage

Following supply voltage is specified at the COM Express® connector:

|          |              |
|----------|--------------|
| VCC:     | 8.5V - 20V   |
| Standby: | 5V DC +/- 5% |
| RTC:     | 2.5V - 3.47V |



- 5V Standby voltage is not mandatory for operation.
- Extended Temperature (E1) variants are validated for 12V supply only

### 3.5.2 Power Supply Rise Time

- » The input voltages shall rise from  $\leq 10\%$  of nominal to within the regulation ranges within 0.1ms to 20ms.
- » There must be a smooth and continuous ramp of each DC input voltage from 10% to 90% of its final set-point following the ATX specification

### 3.5.3 Supply Voltage Ripple

- » Maximum 100 mV peak to peak 0 – 20 MHz

### 3.5.4 Power Consumption

The maximum Power Consumption of the different COMe-bHL6 variants is 17 - 48W (100% CPU load on all cores; 90°C CPU temperature). Further information with detailed measurements are available in Application Note KEMAP054 available on [EMD Customer Section](#). Information there is available after registration.

### 3.5.5 ATX Mode

By connecting an ATX power supply with VCC and 5VSB, PWR\_OK is set to low level and VCC is off. Press the Power Button to enable the ATX PSU setting PWR\_OK to high level and powering on VCC. The ATX PSU is controlled by the PS\_ON# signal which is generated by SUS\_S3# via inversion. VCC can be 8.5V - 20V in ATX Mode. On Computer-on-Modules supporting a wide range input down to 4.75V the input voltage shall always be higher than 5V Standby (VCC > 5VSB).

| State   | PWRBTN#      | PWR_OK     | V5_StdBy | PS_ON#     | VCC       |
|---------|--------------|------------|----------|------------|-----------|
| G3      | x            | x          | 0V       | x          | 0V        |
| S5      | high         | low        | 5V       | high       | 0V        |
| S5 → S0 | PWRBTN Event | low → high | 5V       | high → low | 0 V → VCC |
| S0      | high         | high       | 5V       | low        | VCC       |

### 3.5.6 Single Supply Mode

In single supply mode (or automatic power on after power loss) without 5V Standby the module will start automatically when VCC power is connected and Power Good input is open or at high level (internal PU to 3.3V). PS\_ON# is not used in this mode and VCC can be 8.5V - 20V.

To power on the module from S5 state press the power button or reconnect VCC. Suspend/Standby States are not supported in Single Supply Mode.

| State   | PWRBTN#      | PWR_OK      | V5_StdBy | VCC              |
|---------|--------------|-------------|----------|------------------|
| G3      | x            | x           | x        | 0                |
| G3 → S0 | high         | open / high | x        | connecting VCC   |
| S5      | high         | open / high | x        | VCC              |
| S5 → S0 | PWRBTN Event | open / high | x        | reconnecting VCC |



Signals marked with “x” are not important for the specific power state. There is no difference if connected or open.

All ground pins have to be tied to the ground plane of the carrier board.



## 3.6 Power Control

### Power Supply

The COMe-bHL6 supports a power input from 8.5V - 20V. The supply voltage is applied through the VCC pins (VCC) of the module connector.

### Power Button (PWRBTN#)

The power button (Pin B12) is available through the module connector described in the pinout list. To start the module via Power Button the PWRBTN# signal must be at least 50ms ( $50\text{ms} \leq t < 4\text{s}$ , typical 400ms) at low level (Power Button Event).

Pressing the power button for at least 4seconds will turn off power to the module (Power Button Override).

### Power Good (PWR\_OK)

The COMe-bHL6 provides an external input for a power-good signal (Pin B24). The implementation of this subsystem complies with the COM Express® Specification. PWR\_OK is internally pulled up to 3.3V and must be high level to power on the module.

### Reset Button (SYS\_RESET#)

The reset button (Pin B49) is available through the module connector described in the pinout list. The module will stay in reset as long as SYS\_RESET# is grounded. If available, the BIOS setting for "Reset Behavior" must be set to "Power Cycle".



Modules with Intel® Chipset and active Management Engine do not allow to hold the module in Reset out of S0 for a long time. At about 10s holding the reset button the ME will reboot the module automatically

### SM-Bus Alert (SMB\_ALERT#)

With an external battery manager present and SMB\_ALERT# (Pin B15) connected the module always powers on even if BIOS switch "After Power Fail" is set to "Stay Off".

## 3.7 Environmental Specification

### 3.7.1 Temperature Specification

Kontron defines following temperature grades for Computer-on-Modules in general. Please see chapter 'Product Specification' for available temperature grades for the COMe-bHL6

| Temperature Specification                 | Operating      | Non-operating  | Validated Input Voltage |
|---|----------------|----------------|-------------------------|
| Commercial grade                          | 0°C to +60°C   | -30°C to +85°C | VCC: 8.5V - 20V         |
| Extended Temperature (E1)                 | -25°C to +75°C | -30°C to +85°C | VCC: 12V                |
| Industrial grade by <b>Screening</b> (XT) | -40°C to +85°C | -40°C to +85°C | VCC: 12V                |
| Industrial grade by <b>Design</b> (E2)    | -40°C to +85°C | -40°C to +85°C | VCC: 8.5V - 20V         |

#### Operating with Kontron heatspreader plate assembly

The operating temperature defines two requirements:

- » the maximum ambient temperature with ambient being the air surrounding the module.
- » the maximum measurable temperature on any spot on the heatspreader's surface

#### Test specification:

| Temperature Grade                         | Validation requirements   |
|---|---|
| Commercial grade                          | at 60°C HSP temperature the CPU @ 100% load needs to run at nominal frequency                       |
| Extended Temperature (E1)                 | at 75°C HSP temperature the CPU @ 75% load is allowed to start speedstepping for thermal protection |
| Industrial grade by <b>Screening</b> (XT) | at 85°C HSP temperature the CPU @ 50% load is allowed to start throttling for thermal protection    |
| Industrial grade by <b>Design</b> (E2)    | at 85°C HSP temperature the CPU @ 50% load is allowed to start throttling for thermal protection    |

#### Operating without Kontron heatspreader plate assembly

The operating temperature is the maximum measurable temperature on any spot on the module's surface.

### 3.7.2 Humidity

- » 93% relative Humidity at 40°C, non-condensing (according to IEC 60068-2-78)

## 3.8 Standards and Certifications

### RoHS II

The **COMe-bHL6** is compliant to the directive 2011/65/EU on the Restriction of the use of certain Hazardous Substances (RoHS II) in electrical and electronic equipment



### Component Recognition UL 60950-1

The **COM Express® basic** form factor Computer-on-Modules are Recognized by Underwriters Laboratories Inc. Representative samples of this component have been evaluated by UL and meet applicable UL requirements.

UL Listings:

- » [NWGQ2.E304278](#)
- » [NWGQ8.E304278](#)



### WEEE Directive

WEEE Directive 2002/96/EC is not applicable for Computer-on-Modules.

### Conformal Coating

Conformal Coating is available for Kontron Computer-on-Modules and for validated SO-DIMM memory modules. Please contact your local sales or support for further details.

### Shock & Vibration

The **COM Express® basic** form factor Computer-on-Modules successfully passed shock and vibration tests according to

- » IEC/EN 60068-2-6 (Non operating Vibration, sinusoidal, 10Hz-4000Hz, +/-0.15mm, 2g)
- » IEC/EN 60068-2-27 (Non operating Shock Test, half-sinusoidal, 11ms, 15g)

### EMC

Validated in Kontron reference housing for EMC the **COMe-bHL6** follows the requirements for electromagnetic compatibility standards

- » EN55022

### 3.9 MTBF

The following MTBF (Mean Time Before Failure) values were calculated using a combination of manufacturer's test data, if the data was available, and the Telcordia (Bellcore) issue 2 calculation for the remaining parts.

The calculation method used is "Telcordia Issue 2 Method 1 Case 3" in a ground benign, controlled environment (GB,GC). This particular method takes into account varying temperature and stress data and the system is assumed to have not been burned in.

Other environmental stresses (extreme altitude, vibration, salt water exposure, etc) lower MTBF values.

System MTBF (hours): 215836 @ 40°C (w/PCB)



Fans usually shipped with Kontron products have 50,000-hour typical operating life. The above estimates assume no fan, but a passive heat sinking arrangement Estimated RTC battery life (as opposed to battery failures) is not accounted for in the above figures and need to be considered separately. Battery life depends on both temperature and operating conditions. When the Kontron unit has external power; the only battery drain is from leakage paths.



## 3.10 Mechanical Specification

### Dimension

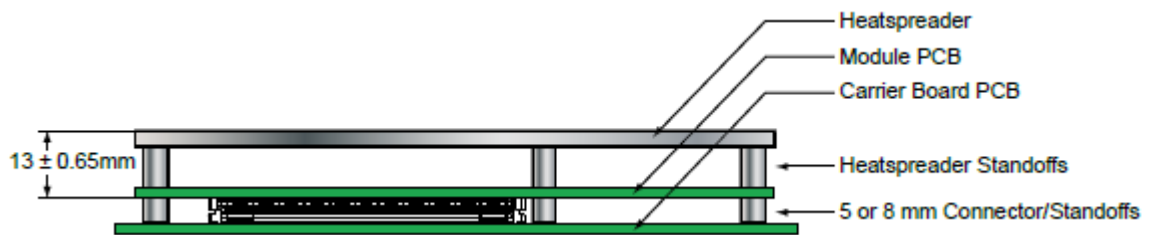
- » 95.0 mm x 125.0 mm
- » Height approx. 12mm (0.4")



CAD drawings are available at [EMD CustomerSection](#)

### Height

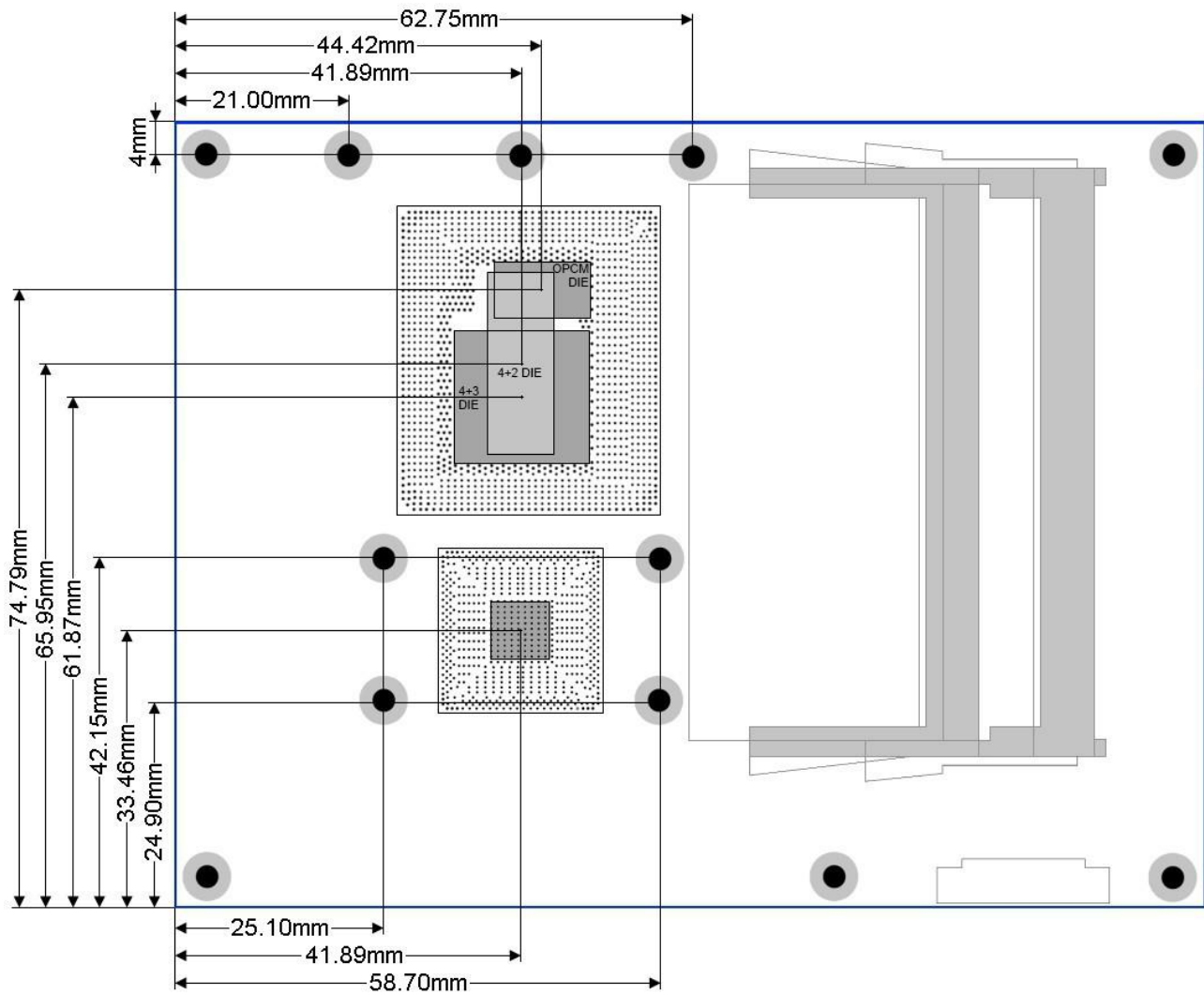
The COM Express® specification defines a module height of 13mm from module PCB bottom to heatspreader top:



Cooling solutions provided from Kontron for basic sized Computer-on-Modules are 27mm in height from module bottom to Heatsink top.

Universal Cooling solutions to be mounted on the HSP (36099-0000-00-x) are 14.3mm in height for an overall height of 27.3mm from module bottom to Heatsink top.

### 3.11 Module Dimensions



4+2 DIE: CPU with GT1 or GT2 graphics  
 4+3 DIE: CPU with GT3 graphics  
 OPCM DIE: eDRAM for GT3 graphics

## 3.12 Thermal Management, Heatspreader and Cooling Solutions

A heatspreader plate assembly is available from Kontron for the COMe-bHL6. The heatspreader plate on top of this assembly is NOT a heat sink. It works as a COM Express®-standard thermal interface to use with a heat sink or external cooling devices.

External cooling must be provided to maintain the heatspreader plate at proper operating temperatures. Under worst-case conditions, the cooling mechanism must maintain an ambient air and heatspreader plate temperature on any spot of the heatspreader's surface according the module specifications:

- » 60°C for commercial grade modules
- » 75°C for extended temperature grade modules (E1)
- » 85°C for industrial temperature grade modules (E2/XT)

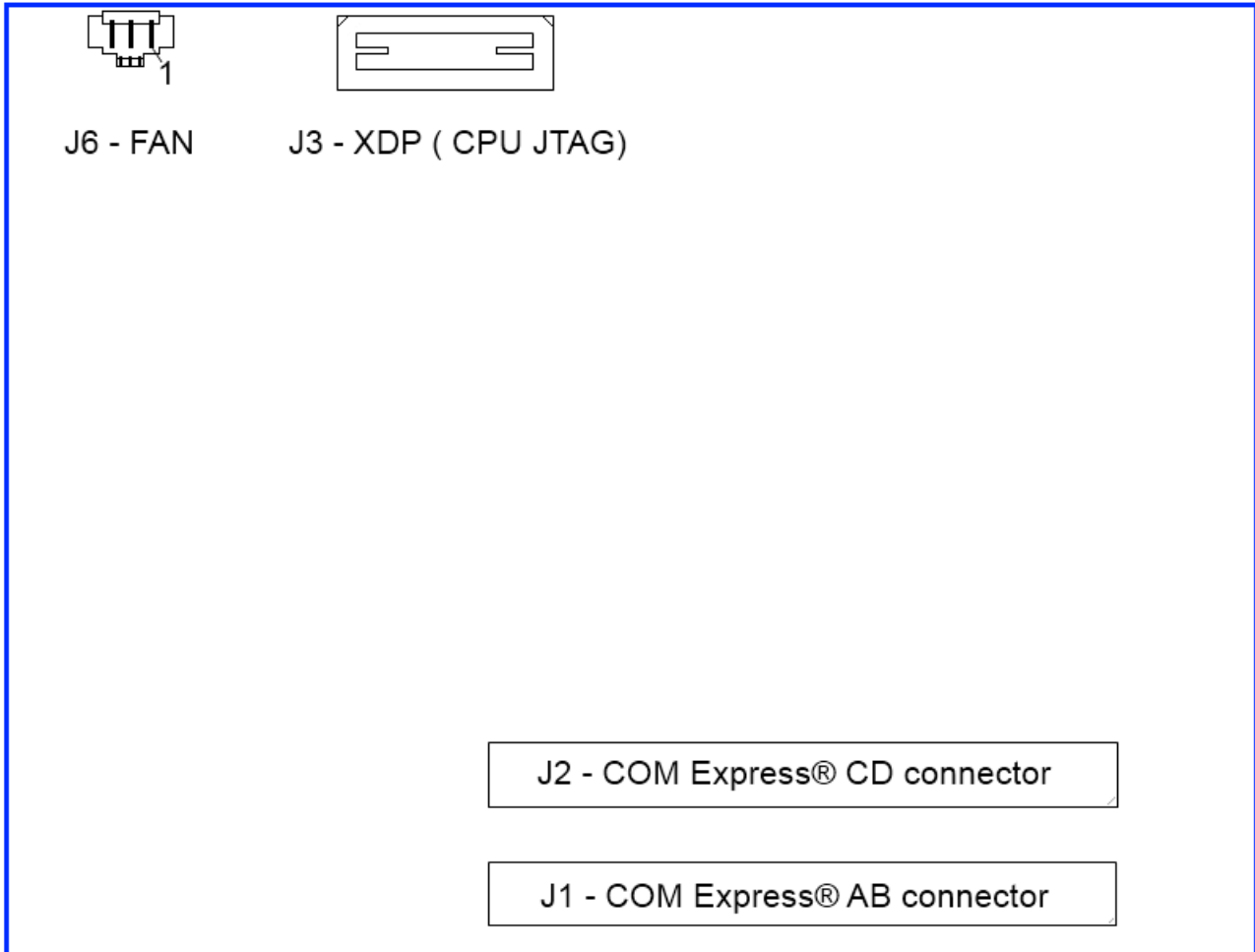
The aluminum slugs and thermal pads or the heat-pipe on the underside of the heatspreader assembly implement thermal interfaces between the heatspreader plate and the major heat-generating components on the COMe-bHL6. About 80 percent of the power dissipated within the module is conducted to the heatspreader plate and can be removed by the cooling solution.

You can use many thermal-management solutions with the heatspreader plates, including active and passive approaches. The optimum cooling solution varies, depending on the COM Express® application and environmental conditions. Active or passive cooling solutions provided from Kontron for the COMe-bHL6 are usually designed to cover the power and thermal dissipation for a commercial grade temperature range used in a housing with proper air flow.

Documentation and CAD drawings of COMe-bHL6 heatspreader and cooling solutions are provided at <http://emdcustomersection.kontron.com>.



### 3.13 Onboard Connectors



#### 3.13.1 FAN Connector J6 - PCB bottom

##### Specification

- » Part number (Molex) J8: 53261-0371
- » Mates with: 51021-0300
- » Crimp terminals: 50079-8100

##### Pin assignment

- » Pin1: Tacho, Pin2: VCC, Pin3: GND

##### Electrical characteristic

| Module Input Voltage    | 8.5 - 13V | 13 - 20V |
|-------------------------|-----------|----------|
| FAN Output Voltage      | 8.5 - 13V | 13V      |
| Max. FAN Output Current | 350mA     | 150mA    |



To connect a standard FAN with 3pin connector to the module please use adaptor cable KAB-HSP 200mm (96079-0000-00-0) or KAB-HSP 40mm (96079-0000-00-2)

### **3.13.2 CPU JTAG connector J3 - PCB bottom**

The XDP connector is for internal use only. Do not use under any circumstances

### **3.13.3 CPLD Debug connector J7 - PCB top**

The CPLD Debug and programming connector is for internal use only. Do not use under any circumstances

## 4 Features and Interfaces

### 4.1 S5 Eco Mode

Kontron's new high-efficient power-off state S5 Eco enables lowest power-consumption in soft-off state – less than 1 mA compared to the regular S5 state this means a reduction by at least factor 200!

In the "normal" S5 mode the board is supplied by 5V\_Stb and needs usually up to 300mA just to stay off. This mode allows to be switched on by power button, RTC event and WakeOnLan, even when it is not necessary. The new S5 Eco mode reduces the current enormous.

The S5 Eco Mode can be enabled in BIOS Setup, when the BIOS supports this feature.

Following prerequisites and consequences occur when S5 Eco Mode is enabled

- » The power button must be pressed at least for 200ms to switch on.
- » Wake via Power button only.
- » "Power On After Power Fail"/"State after G3": only "stay off" is possible

### 4.2 Rapid Shutdown

#### Overview

For "R" or the "RXT" version of the COMe-bHL6, Kontron has implemented a rapid shutdown function. It works as follows:

1) An active-high shutdown signal is asserted by the COM Express Eval Type 2 carrier board via pin C67 of the COM Express connector. The characteristics of the shutdown signal are as follows:

- » Amplitude 5.0V +/- 5%
- » Source impedance  $\leq 50$  ohms
- » Rise time  $\leq 1\mu\text{s}$
- » Duration  $\geq 20\mu\text{s}$

The assertion of this signal causes all power regulators to be disabled and the internal power supply rails to be discharged by crowbar circuits. The shutdown circuitry provides internal energy storage that maintains crowbar activation for at least 2mS following the de-assertion of the shutdown signal. The circuit also incorporates a weak input pulldown resistor so that the RXT module will operate normally in systems where the rapid shutdown functionality is not used and pin C67 of the COM Express is left unconnected.

2) Simultaneously with the leading edge of shutdown, the 12V (main) input power to the RXT module is removed and these input power pins are externally clamped to ground through a crowbar circuit located on the COM Express carrier board. This external clamping circuit must maintain a maximum resistance of approximately 1 ohm and be activated for a minimum of 2mS.

3) Simultaneously with the leading edge of shutdown, the 5V (standby) input power to the RXT module is removed, if present. External clamping on these pins is not necessary.

#### Crowbar implementation details

As a tool for designing the internal crowbars, Kontron developed tallied the total capacitance present on each of the internal power rails, and calculates the required discharge resistance in order to achieve the desired voltage decay time constant. The principal design criteria are that each supply rail must decay to 37% of initial value (equivalent to 1RC) within 250uS, and to below 1.5V within 2mS. Analysis shows that the power rails fall into four general classes. Each class of power rails has a corresponding discharge strategy.

1) Power Input Rails: The main 12V power input rail incorporates about 300uF of distributed capacitance. This rail must be discharged by an external crowbar located on the carrier board, which must provide a shunt resistance of approximately 1 ohm. The peak power dissipation in this crowbar resistance will be relatively high (on the order of 150W when the crowbar is activated), but will diminish very rapidly as the input capacitors discharge.

2) Low Voltage, High Power Rails: Each of these 5 “major” internal supply rails has an output voltage in the 1.0 V to 1.5V range, and each rail has between 1500uF and 3300uF of output capacitance. The required discharge resistances for these rails are in the range of 0.1 to 0.2 ohm, and peak discharge currents are in the range of 8 to 16A.

The discharge circuit for each rail is implemented with a “pulse withstanding” thick-film SMT resistor in series with a low-RDSon MOSFET. The resistor peak powers are in the 8W to 20W range; depending on PCB layout considerations either a single resistor or multiple smaller resistors may be used to achieve sufficient pulse handling capability.

Because of the relatively high currents in the discharge paths, these crowbar circuits require wide copper traces and careful component placement adjacent to the output components of the corresponding power supplies.

3) Low Voltage, Low Power Rails: These rails have voltages of 1.8V or less and capacitances under 1000uF, with peak discharge currents <3A. The discharge circuits for these rails are also implemented with resistor(s) and a low-RDSon

4) MOSFET. In some cases, the peak pulse power dissipation in the resistor(s) is low enough that specialty “pulse withstanding” resistors are not required.

5) Medium Voltage Rails: These 3.3V and 5V rails typically have relatively small output capacitances and peak discharge currents <1A. The discharge circuits for these rails are typically implemented with conventional resistor(s) and a low-RDSon MOSFET.

### Shutdown input circuit details

The shutdown input pin to the RXT module is coupled through a series Schottky diode and a small series resistor to the gates of all crowbar MOSFETs, connected in parallel. All crowbar MOSFETs are N-channel “logic level” parts that have are specified for operation at  $V_{gs} = 4.5V$ . Three additional components are connected in parallel between the MOSFET gates and ground:

- » A capacitor that provides energy storage to keep the MOSFETs conducting for several mS after the shutdown signal is de-asserted.
- » A high-value resistor that provides a discharge path for the capacitor as well as a pulldown resistance (to insure that the shutdown circuits remain inactive if the shutdown pin is left floating).
- » A 6.2V zener diode that protects the MOSFET gates from damage due to input ESD or input overdrive.

In order to insure that the crowbars do not “fight” active switching regulators while the input capacitors are being discharged, the shutdown circuit rapidly crowbars the 5V rail, with a time constant <10uS. The 5V rail powers most of the remaining switching regulators, and as its voltage falls below about 4V those regulators enter under-voltage lockout mode and cease to operate. Additionally, by using the UVLO mechanism in the design of the RXT module, Kontron minimizes the risk of inadvertently affecting the standard power sequencing logic for such RXT modules. Two of the switching regulators do not require the 5V supply for operation, and in those two cases it will be necessary to clamp the enable inputs to ground when shutdown begins.

## 4.3 LPC

The Low Pin Count (LPC) Interface signals are connected to the LPC Bus bridge located in the CPU or chipset. The LPC low speed interface can be used for peripheral circuits such as an external Super I/O Controller, which typically combines legacy-device support into a single IC. The implementation of this subsystem complies with the COM Express® Specification. Implementation information is provided in the COM Express® Design Guide maintained by PICMG. Please refer to the official PICMG documentation for additional information.

The LPC bus does not support DMA (Direct Memory Access) and a clock buffer is required when more than one device is

used on LPC. This leads to limitations for ISA bus and SIO (standard I/O's like Floppy or LPT interfaces) implementations.

All Kontron COM Express® Computer-on-Modules imply BIOS support for following external baseboard LPC Super I/O controller features for the **Winbond/Nuvoton 5V 83627HF/G and 3.3V 83627DHG-P**:

| 83627HF/G  | Phoenix BIOS | AMI CORE8 | AMI / Phoenix EFI |
|------------|--------------|-----------|-------------------|
| PS/2       | YES          | YES       | YES               |
| COM1/COM2  | YES          | YES       | YES               |
| LPT        | YES          | YES       | YES               |
| HWM        | YES          | YES       | NO                |
| Floppy     | NO           | NO        | NO                |
| GPIO       | NO           | NO        | NO                |
| 83627DHG-P | Phoenix BIOS | AMI CORE8 | AMI / Phoenix EFI |
| PS/2       | YES          | YES       | YES               |
| COM1/COM2  | YES          | YES       | YES               |
| LPT        | YES          | YES       | YES               |
| HWM        | NO           | NO        | NO                |
| Floppy     | NO           | NO        | NO                |
| GPIO       | NO           | NO        | NO                |

Features marked as not supported do not exclude OS support (e.g. HWM can be accessed via SMB). For any other LPC Super I/O additional BIOS implementations are necessary. Please contact your local sales or support for further details.

## 4.4 Serial Peripheral Interface (SPI)

The Serial Peripheral Interface Bus or SPI bus is a synchronous serial data link standard named by Motorola that operates in full duplex mode. Devices communicate in master/slave mode where the master device initiates the data frame. Multiple slave devices are allowed with individual slave select (chip select) lines. Sometimes SPI is called a “four wire” serial bus, contrasting with three, two, and one wire serial buses.



The SPI interface can only be used with a SPI flash device to boot from external BIOS on the baseboard.

## 4.5 SPI boot

The COMe-bHL6 supports boot from an external SPI Flash. It can be configured by pin A34 (BIOS\_DIS#0) and pin B88 (BIOS\_DIS1#) in following configuration:

| BIOS_DIS0# | BIOS_DIS1# | Function   |
|------------|------------|--|
| open       | open       | Boot on-module BIOS  |
| GND        | open       | Boot baseboard LPC FWH                                       |
| open       | GND        | Baseboard SPI = Boot Device 1, on-module SPI = Boot Device 2 |
| GND        | GND        | Baseboard SPI = Boot Device 2, on-module SPI = Boot Device 1 |



By default only SPI Boot Device 1 is used in configuration 3 & 4. Both SPI Boot Devices are used by splitting the BIOS with modified descriptor table in customized versions only

### Recommended SPI boot flash types for 8-SOIC package

| Size     | Vendor            | Vendor ID | Part Number        | Device ID                         |
|----------|-------------------|-----------|--------------------|-----------------------------------|
| 128 Mbit | Macronix          | 0xC2      | MX25L12835FM2I-10G | Device ID0 0x20 / Device ID1 0x18 |
| 128 Mbit | Micron Technology | 0x20      | N25Q128A13ESE40F   | Device ID0 0xBA / Device ID1 0x18 |
| 128 Mbit | Micron Technology | 0x20      | N25Q128A13ESE40E   | Device ID0 0xBA / Device ID1 0x18 |
| 128 Mbit | Winbond           | 0xEF      | W25Q128FVSIQ       | Device ID0 0x40 / Device ID1 0x18 |
| 128 Mbit | Winbond           | 0xEF      | W25Q128JVSQTR      | Device ID0 0x40 / Device ID1 0x18 |
| 128 Mbit | Winbond           | 0xEF      | W25Q128JVSQ        | Device ID0 0x40 / Device ID1 0x18 |

## Using an external SPI flash

To program an external SPI flash follow these steps:

- » Connect a SPI flash with correct size (similar to BIOS ROM file size) to the module SPI interface
- » Open pin A34 and B88 to boot from the module BIOS
- » Boot the module to DOS/EFI-Shell with access to the BIOS image and Firmware Update Utility provided on EMD Customer Section
- » Connect pin B88 (BIOS\_DIS1#) to ground to enable the external SPI flash
- » Execute Flash.bat/Flash.efi to program the complete BIOS image to the external SPI flash
- » reboot

Your module will now boot from the external SPI flash when BIOS\_DIS1# is grounded.

## External SPI flash on Modules with Intel® ME

If booting from the external (baseboard mounted) SPI flash then exchanging the COM Express® module for another one of the same type will cause the Intel® Management Engine to fail during next start. This is by design of the ME because it bounds itself to the very module it has been flashed to. In the case of an external SPI flash this is the module present at flash time.

To avoid this issue please make sure to conduct a complete flash of the external SPI flash device after changing the COMexpress module for another one. If disconnecting and reconnecting the same module again this step is not necessary.

## 4.6 M.A.R.S.

The Smart Battery implementation for Kontron Computer-on-Modules called **Mobile Application for Rechargeable Systems** is a BIOS extension for external Smart Battery Manager or Charger. It includes support for SMBus charger/selector (e.g. Linear Technology LTC1760 Dual Smart Battery System Manager) and provides ACPI compatibility to report battery information to the Operating System.

Reserved SM-Bus addresses for Smart Battery Solutions on the carrier:

| 8-bit Address | 7-bit Address | Device         |
|---------------|---------------|----------------|
| 12h           | 0x09          | SMART_CHARGER  |
| 14h           | 0x0A          | SMART_SELECTOR |
| 16h           | 0x0B          | SMART_BATTERY  |

## 4.7 UART

The COMe-bHL6 supports up to two Serial RX/TX only Ports defined in COM Express® specification on Pins A98/A99 for UART0 and Pins A101/A102 for UART1. The implementation of the UART is compatible to 16450 and is supported by default from most operating systems. Resources are subordinated to other UARTS e.g. from external LPC Super I/O.

### UART features:

- » 450 to 115.2k Baud (except 56000)
- » 5, 6, 7 or 8bit characters
- » 1 or 2 Stop bit generation
- » Even, odd or no-parity generation/detection
- » Complete status reporting capabilities

- » Line break generation and detection
- » Full prioritized interrupt system control
- » No FIFO
- » One additional shift register for transmit and one for receive
- » No Flow Control
- » No FCR register due to unavailability of FIFO
- » MCR and MSR registers only implemented in loopback mode for compatibility with existing drivers and APIs
- » Initialized per default to COM3 3F8h/IRQ4 and COM4 2F8/IRQ3 without external SIO
- » Initialized per default to COM3 3E8h/IRQ5 and COM4 2E8/IRQ10 with external SIO present

The UART clock is generated by the 33MHz LPC clock which results in an accuracy of 0.5% on all UART timings

- Due to the protection circuitry required according COM Express® specification the transfer speed can only be guaranteed for 9600 Baud. Please contact your local sales or support for customized versions without protection circuitry



- Legacy console redirection via onboard serial ports may be restricted in terms of serial input stream. Since they're only emulating a 16450 device (w/o FIFO) an input stream generated by a program may lose characters. Inputs from a keyboard via terminal program will be safe.

## 4.8 Fast I2C

The COMe-bHL6 supports a CPLD implemented LPC to I2C bridge using the WISHBONE I2C Master Core provided from opencores.org. The I2C Interface supports transfer rates up to 40kB/s and can be configured in Setup

Specification for external I2C:

- » Speed up to 400kHz
- » Compatible to Philips I2C bus standard
- » Multi-Master capable
- » Clock stretching support and wait state generation
- » Interrupt or bit-polling driven byte-by-byte data-transfers
- » Arbitration lost interrupt with automatic transfer cancellation
- » Start/Stop signal generation/detection
- » Bus busy detection
- » 7bit and 10bit addressing

## 4.9 Dual Staged Watchdog Timer

### Basics

A watchdog timer (or computer operating properly (COP) timer) is a computer hardware or software timer that triggers a system reset or other corrective action if the main program, due to some fault condition, such as a hang, neglects to regularly service the watchdog (writing a "service pulse" to it, also referred to as "kicking the dog", "petting the dog", "feeding the watchdog" or "triggering the watchdog"). The intention is to bring the system back from the nonresponsive state into normal operation.

The COMe-bHL6 offers a watchdog which works with two stages that can be programmed independently and used one by one.

### Time-out events

|                        |   |
|------------------------|---|
| <b>Reset</b>           | A reset will restart the module and starts POST and operating system new.   |
| <b>NMI</b>             | A non-maskable interrupt (NMI) is a computer processor interrupt that cannot be ignored by standard interrupt masking techniques in the system. It is typically used to signal attention for non-recoverable hardware errors. |
| <b>SCI</b>             | A system control interrupt (SCI) is a OS-visible interrupt to be handled by the OS using AML code   |
| <b>Delay</b>           | Might be necessary when an operating system must be started and the time for the first trigger pulse must extended. (Only available in the first stage)   |
| <b>WDT Signal only</b> | This setting triggers the WDT Pin on baseboard connector (COM Express® Pin B27) only  |
| <b>Cascade:</b>        | Does nothing, but enables the 2nd stage after the entered time-out.   |

### WDT Signal

B27 on COM Express® Connector offers a signal that can be asserted when a watchdog timer has not been triggered within time. It can be configured to any of the 2 stages. Deassertion of the signal is automatically done after reset. If deassertion during runtime is necessary please ask your Kontron technical support for further help.

## 4.10 Intel® Fast Flash Standby™ / Rapid Start Technology™

The target of Intel® Fast Flash Standby™ (iFFS) (also known as Intel® Rapid Start Technology™ iRST) is to get a wake-up time from S4 comparable to S3. Normally S4 is caused by OS which stores it's information to the hard disk and does then a normal shutdown. S4 resume takes quite long as the system does a normal BIOS POST and OS restores it's information from the hard disk.

iFFS does it in a different way. The Operating System initiates an S3 and stores it's information in memory. After that BIOS copies this OS information from DRAM to SSD and does a sleep state similar to S4 with nearly zero power. If system is resumed by power button, BIOS restores memory content from SSD to the DRAM and does an S3 resume which is much faster.

### Requirements

- » SATA Solid State Disk in AHCI mode
- » Free disk space on the SSD with at least the DRAM size
- » Operating System with disk partition tool to allocate the hibernation partition (e.g. Windows 7/8)
- » BIOS supporting iFFS feature

### How to setup once the operating system is installed

- » Prepare a free disk space on your onboard or external SSD with at least the size of DRAM
- » Open *cmd.exe* in Administrator Mode and type *diskpart.exe* to open the Windows disk partition tool
- » DISKPART> list disk
- » DISKPART> select disk X (X is disk number where you want to create the store partition. Refer to results from "list



disk" for exact disk number)

- » DISKPART> create partition primary
- » DISKPART> detail disk
- » DISKPART> select Volume X (X is Volume of your store partition. Refer to results from "detail disk" for exact volume number)
- » DISKPART> set id=84 override (ID 84 marks the partition as hibernate partition)
- » DISKPART> exit
- » Now there should be a Hibernate Partition visible in your disk management
- » Reboot and enable iFFS in BIOS

### Usage

- » Activate Lid / move system to Sleep/Standby (→S3)
- » After configured period of time in Setup the system powers on automatically and information in DRAM moves to non-volatile memory (Default is 'immediately')
- » System switches off again to iFFS (→comparable to S4, Power Supply can now be disconnected)
- » When System is powered on, information moved back to DRAM (No display output during copy process)
- » System resumes same as Sleep/Standby S3

### Note

- » Depending on the platform iFFS enabled may disable the hibernate function in Windows automatically

### Benefits

- » System transitions from S3 to S4 automatically
- » Up to 6x battery life compared to Standby
- » Resume time reduced up to 75%



Measured resume times from Power-on to Win7 Log-on Screen on COMe-mCT10:

- » 2.5" SATA II HDD 5400rpm: Hibernate: 22s, iFFs on onboard NANDrive: 17s
- » 2.5" SATA III SSD: Hibernate: 18s, iFFS on SSD: 10s

## 4.11 Speedstep Technology

The Intel® processors offer the Intel® Enhanced SpeedStep™ technology that automatically switches between maximum performance mode and battery-optimized mode, depending on the needs of the application being run. It enables you to adapt high performance computing on your applications. When powered by a battery or running in idle mode, the processor drops to lower frequencies (by changing the CPU ratios) and voltage, conserving battery life while maintaining a high level of performance. The frequency is set back automatically to the high frequency, allowing you to customize performance.

In order to use the Intel® Enhanced SpeedStep™ technology the operating system must support SpeedStep™ technology.

By deactivating the SpeedStep feature in the BIOS, manual control/modification of CPU performance is possible. Setup the CPU Performance State in the BIOS Setup or use 3rd party software to control CPU Performance States.

## 4.12 C-States

New generation platforms include power saving features like SuperLFM, EIST (P-States) or C-States in O/S idle mode.

Activated C-States are able to dramatically decrease power consumption in idle mode by reducing the Core Voltage or switching of parts of the CPU Core, the Core Clocks or the CPU Cache.

Following C-States are defined:

| C-State | Description           | Function   |
|---------|-----------------------|--|
| C0      | Operating             | CPU fully turned on  |
| C1      | Halt State            | Stops CPU main internal clocks via software                      |
| C1E     | Enhanced Halt         | Similar to C1, additionally reduces CPU voltage                  |
| C2      | Stop Grant            | Stops CPU internal and external clocks via hardware              |
| C2E     | Extended Stop Grant   | Similar to C2, additionally reduces CPU voltage                  |
| C3      | Deep Sleep            | Stops all CPU internal and external clocks                       |
| C3E     | Extended Stop Grant   | Similar to C3, additionally reduces CPU voltage                  |
| C4      | Deeper Sleep          | Reduces CPU voltage  |
| C4E     | Enhanced Deeper Sleep | Reduces CPU voltage even more and turns off the memory cache     |
| C6      | Deep Power Down       | Reduces the CPU internal voltage to any value, including 0V      |
| C7      | Deep Power Down       | Similar to C6, additionally LLC (LastLevelCache) is switched off |

C-States are usually enabled by default for low power consumption, but active C-States may influence performance sensitive applications or real-time systems.

- » Active C6-State may influence data transfer on external Serial Ports
- » Active C7-State may cause lower CPU and Graphics performance

It's recommended to disable C-States / Enhanced C-States in BIOS Setup if any problems occur.

## 4.13 Hyper Threading

Hyper Threading (officially termed Hyper Threading Technology or HTT) is an Intel®-proprietary technology used to improve parallelization of computations performed on PC's. Hyper-Threading works by duplicating certain sections of the processor—those that store the architectural state but not duplicating the main execution resources. This allows a Hyper-Threading equipped processor to pretend to be two “logical” processors to the host operating system, allowing the operating system to schedule two threads or processes simultaneously. Hyper Threading Technology support always relies on the Operating System.

## 4.14 Dynamic FSB Frequency Switching

Dynamic FSB frequency switching effectively reduces the internal bus clock frequency by half to further decrease the minimum processor operating frequency from the Enhanced Intel SpeedStep Technology performance states and achieve the Super Low Frequency Mode (Super LFM). This feature is supported at FSB frequencies of 1066 MHz, 800 MHz and 667 MHz and does not entail a change in the external bus signal (BCLK) frequency. Instead, both the processor and GMCH internally lower their BCLK reference frequency to 50% of the externally visible frequency. Both the processor and GMCH maintain a virtual BCLK signal (VBCLK) that is aligned to the external BCLK but at half the frequency.

After a downward shift, it would appear externally as if the bus is running with a 133-MHz base clock in all aspects, except that the actual external BCLK remains at 266 MHz. See Figure 3 for details. The transition into Super LFM, a “down-shift,” is done following a handshake between the processor and GMCH. A similar handshake is used to indicate an “up-shift,” a change back to normal operating mode. Please ensure this feature is enabled and supported in the BIOS.

## 4.15 VID-x

The processor implements the VID-x feature for improved control of core voltage levels when the processor enters a reduced power consumption state. VID-x applies only when the processor is in the Intel Dynamic Acceleration Technology performance state and one or more cores are in low-power state (i.e., CC3/CC4/CC6). VID-x provides the ability for the processor to request core voltage level reductions greater than one VID tick. The amount of VID tick reduction is fixed and only occurs while the processor is in Intel Dynamic Acceleration Technology mode. This improved voltage regulator efficiency during periods of reduced power consumption allows for leakage current reduction which results in platform power savings and extended battery life.

When in Intel Dynamic Acceleration Technology mode, it is possible for both cores to be active under certain internal conditions. In such a scenario the processor may draw an Instantaneous current (ICC\_CORE\_INST) for a short duration of tINST; however, the average ICC current will be lesser than or equal to ICCDES current specification.

## 4.16 Intel® Turbo Boost Technology and AVX

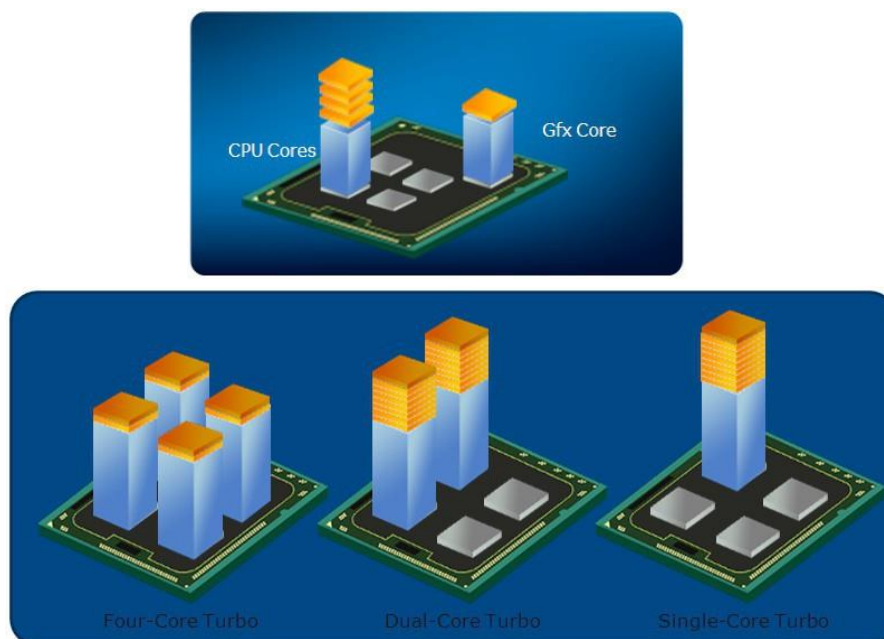
For applications that are particularly power-hungry, the new processors provide enhanced Intel® Turbo Boost technology. This automatically shifts processor cores and processor graphics resources to accelerate performance, tailoring a workload to give users an immediate performance boost for their applications whenever needed. Another innovation is the enhancement to the 256-bit instruction set, known as Intel® Advanced Vector Extensions (AVX). AVX delivers improved performance, rich functionality and the ability to manage, rearrange and sort data in a better way. The new instruction set accelerates floating-point intensive applications such as “number crunchers” or digital processing of images, videos and audio data.

### Intel® Turbo Boost Technology 2.0

Intel has optimized Intel® Turbo Boost Technology to provide even more performance when needed on the latest-generation Intel® microarchitecture. Intel® Turbo Boost Technology 2.0 automatically allows processor cores to run faster than the base operating frequency if it's operating below power, current, and temperature specification limits. Intel Turbo Boost Technology 2.0 is activated when the Operating System (OS) requests the highest processor performance state (P0).

The maximum frequency of Intel Turbo Boost Technology 2.0 is dependent on the number of active cores. The amount of time the processor spends in the Intel Turbo Boost Technology 2.0 state depends on the workload and operating environment. Any of the following can set the upper limit of Intel Turbo Boost Technology 2.0 on a given workload:

- » Number of active cores
- » Estimated current consumption
- » Estimated power consumption
- » Processor temperature



When the processor is operating below these limits and the user's workload demands additional performance, the processor frequency will dynamically increase until the upper limit of frequency is reached. Intel Turbo Boost Technology 2.0 has multiple algorithms operating in parallel to manage current, power, and temperature to maximize performance and energy efficiency. Note: Intel Turbo Boost Technology 2.0 allows the processor to operate at a power level that is higher than its rated upper power limit (TDP) for short durations to maximize performance.

## 4.17 Display Configuration

### Maximum supported Resolutions in Single Display Configuration

| Port     | Max Resolution  |
|----------|---|
| DP       | 3840×2160@60Hz, 24bpp<br>4096×2160@24Hz, 24bpp                          |
| HDMI     | 4096×2160@24Hz, 24bpp<br>2560×1600@60Hz, 24bpp<br>1920×1080@60Hz, 36bpp |
| DVI      | 1920×1200@60Hz, 24bpp   |
| VGA      | 1920×1200@60Hz, 24bpp   |
| WiDi     | 1920×1080@30Hz, 24bpp<br>1280×720@60Hz, 24bpp                           |
| eDP (x2) | 1920×1200@60Hz  |
| LVDS     | 1920×1200@60Hz  |

### Maximum supported Pixel Clock

| Port | Max Pixel Clock |
|------|-----------------|
| DP   | 533 MHz         |
| HDMI | 300 MHz         |
| DVI  | 165 MHz         |
| VGA  | 180 MHz         |

## DDI supported resolutions in 3 Display Configurations

| Display1 | Display2 | Display3 | Max.Res Display 1                | Max.Res Display 2                | Max.Res Display 3                |
|----------|----------|----------|----------------------------------|----------------------------------|----------------------------------|
| HDMI/DP  | HDMI/DP  | DP       | 4096×2160@24Hz<br>3840×2160@60Hz | 4096×2160@24Hz<br>3840×2160@60Hz | 3840×2160@60Hz                   |
| HDMI/DP  | HDMI/DP  | eDP/LVDS | 4096×2160@24Hz<br>3840×2160@60Hz | 4096×2160@24Hz<br>3840×2160@60Hz | 1920×1200@60Hz                   |
| DP       | DVI/WiDi | DVI      | 3840×2160@60Hz                   | 1920×1200@60Hz<br>1920×1080@30Hz | 1920×1200@60Hz                   |
| eDP/LVDS | DVI/WiDi | DVI      | 1920×1200@60Hz                   | 1920×1200@60Hz<br>1920×1080@30Hz | 1920×1200@60Hz                   |
| VGA/WiDi | DP/HDMI  | DP/HDMI  | 1920×1200@60Hz<br>1920×1080@30Hz | 3840×2160@60Hz<br>4096×2160@24Hz | 3840×2160@60Hz<br>4096×2160@24Hz |
| VGA/WiDi | eDP/LVDS | DP/HDMI  | 1920×1200@60Hz<br>1920×1080@30Hz | 1920×1200@60Hz                   | 3840×2160@60Hz<br>4096×2160@24Hz |
| DP       | DP       | DVI      | 3840×2160@60Hz                   | 3840×2160@60Hz                   | 1920×1200@60Hz                   |
| eDP/LVDS | DP       | DVI      | 1920×1200@60Hz                   | 3840×2160@60Hz                   | 1920×1200@60Hz                   |
| VGA      | DVI      | DVI/WiDi | 1920×1200@60Hz                   | 1920×1200@60Hz                   | 1920×1200@60Hz<br>1920×1080@30Hz |
| VGA      | DP/HDMI  | DVI/WiDi | 1920×1200@60Hz                   | 3840×2160@60Hz<br>4096×2160@24Hz | 1920×1200@60Hz<br>1920×1080@30Hz |
| VGA      | eDP/LVDS | DVI/WiDi | 1920×1200@60Hz                   | 1920×1200@60Hz                   | 1920×1200@60Hz<br>1920×1080@30Hz |
| DVI      | DVI      | WiDi     | 1920×1200@60Hz                   | 1920×1200@60Hz                   | 1920×1080@30Hz                   |

## Link Data Rate

The maximum supported Display Ports resolutions are dependent on the Link Data Rate and the used Lane Count:

| Link Data Rate | 1 Lane    | 2 Lanes   | 4 Lanes   |
|----------------|-----------|-----------|-----------|
| RBR            | 1024×600  | 1400×1050 | 2240×1400 |
| HBR            | 1280×960  | 1920×1200 | 2880×1800 |
| HBR2           | 1920×1200 | 2880×1800 | 3840×2160 |

## 3 independent Display Support

The COMe-bHL6 supports up to 3 independent displays in Windows 7/8 and Linux by using the following rules:

- » Max of 2 HDMI
- » Max of 2 DVI
- » Max of 1 HDMI and 1DVI
- » Any 3 DisplayPort
- » One VGA

## Digital Display Interface Features

The integrated Intel® HD/HD4600/HD5200 (Gen7.5) graphics supports:

- » High-bandwidth Digital Content Protection (HDCP) on HDMI and DisplayPort with up to 2 HDCP streams simultaneously
- » One active Protected Audio and Video Path (PAVP) session on HDMI or DisplayPort
- » Dual Stream DP/HDMI Audio
- » DP/HDMI/DVI Hot-plug (low-active)

## Supported Audio Formats on HDMI and DisplayPort

| Audio Formats                      | HDMI | DisplayPort |
|------------------------------------|------|-------------|
| AC-3 Dolby Digital                 | YES  | YES         |
| Dolby Digital Plus                 | YES  | YES         |
| DTS-HD                             | YES  | YES         |
| LPCM, 192kHz/24bit, 8 channel      | YES  | YES         |
| Dolby True HD, DTS HD Master Audio | YES  | YES         |

## DDI Design Consideration

- » For sufficient signal quality baseboard designs with long signal lanes or impedance leaps may require an Equalizer or Re-driver for the digital display interfaces
- » DDI hot-plug detection is high active
- » DisplayPort can be used directly or with external adapters for HDMI, DVI or VGA
- » HDMI or DVI usage on a baseboard requires a level shifter



Find more details for DDI usage as DisplayPort, HDMI or DVI with schematic examples available on <http://emdcustomersection.kontron.com>

## DVI-I Design Topology

DVI-I is supported on PCH Digital Display Port B (COM DDI1) only. The implementation involves routing VGA and DVI-D signals to DVI-I connector:

- » VGA port RGB signals should be routed to Analog RGB pins on the DVI-I connector
- » DVI Data and Clock signals on PCH Digital Display Port B should be routed to TMDS Data 0, 1 and 2 pins and TMDS Clock pin of DVI-I connector respectively
- » DVI HPD signals should be routed to the HPD pin of the DVI-I connector
- » DVI DDC Clock and Data signals on PCH Digital Display Port B should be routed to the DDC Clock and Data pins of the DVI-I connector.

## 4.18 Hybrid Graphics / Multi-monitor

The COMe-bHL6 supports Hybrid Multi-monitor function which is one form of Intel's Hybrid Graphics where integrated graphics (in Chipset or CPU) is available to operate simultaneously with external PEG; PCIe or PCI graphics. This feature enables concurrent function of Intel's integrated Graphics Processing Unit (GPU/iGFX) along with a discrete GPU solution, allowing for operability of greater than two independently-driven displays. The O/S will handle control of the multiple GPU display adapters appropriately. For example, WindowsXP supports The Microsoft Windows XP Display Driver Model (XPDM) which allows loading and support of multiple graphics drivers. Windows 7 continues that legacy XPDM support but also adds WDDM v1.1 which, like XPDM, allows for simultaneous multiple graphics drivers (Windows Vista WDDM v1.0 did not allow this capability). Operating system applications will be adapter-unaware through use of the O/S GUI APIs and will utilize the adapter associated with the primary display, regardless of which display the image is located on.



Some applications may be adapter-aware, e.g., full-screen applications and system applications like the compositor. A number of software tools designed to assist multi-monitor use are available from third parties. One example is the UltraMon\* utility for multi-monitor systems, which helps with the position of applications, assists desktop wallpapers and screen savers in multi-monitor configurations.

Hybrid Multi-monitor mode is recommended to be accomplished using a discrete third-party PCI Express graphics card either into the PEG slot of the platform or into an available PCI Express slot routed off of the I/O subsection of the chipset.

## Requirements

- » Baseboard supporting PEG (alternatively PCIe or PCI)
- » Module BIOS which allows switching between iGFX and discrete GPU (iGFX must be set to primary boot display)
- » O/S supporting heterogeneous display adapters (Linux / WindowsXP / Windows 7)

## Setup a Multi-monitor system

- » Start without the discrete GPU seated in the system
- » Select IGD as Primary Boot Display in BIOS Setup
- » Boot into O/S and install drivers requested for the integrated GPU
- » Shut down the system and insert the discrete GPU
- » Boot into O/S and install drivers requested for the discrete GPU (if necessary in Safe mode)
- » Set the Windows Display properties as referenced below (example: WindowsXP)



In most cases the graphical user interfaces (e.g. ATI Catalyst Control Center) for both GPUs may not run properly. It's recommended to use O/S implemented Display Properties like in screenshot above



Detailed documentation is available in Intel Paper [323214](#)

## 4.19 Intel® Wireless Display

Intel® Wireless Display, most commonly known as WiDi, is a wireless display standard developed by Intel, based on the existing Wi-Fi standard. It allows a portable device or computer to send up to 1080p HD video and 5.1 surround sound to a compatible display wirelessly.

The COMe-bHL6 supports WiDi in combination with following requirements:

CPU:

- » 2nd Generation Intel® Core(TM) i7/i5/i3
- » 3rd Generation Intel® Core(TM) i7/i5/i3
- » 4th Generation Intel® Core(TM) i7/i5/i3
- » Intel® Celeron N28xx / N29xx Series

One of the following Wireless Devices:

- » Intel® Centrino® Wireless-N 1000, 1030, 2200, or 2230
- » Intel® Centrino® Wireless-N 2200 for Desktop
- » Intel® Centrino® Advanced-N 6200, 6205, 6230, or 6235
- » Intel® Centrino® Advanced-N 6205 for Desktop
- » Intel® Centrino® Wireless-N + WiMAX 6150
- » Intel® Centrino® Advanced-N + WiMAX 6250

- » Intel® Centrino® Ultimate-N 6300
- » Intel® Dual Band Wireless-N 7260
- » Intel® Dual Band Wireless-AC 7260
- » Intel® Dual Band Wireless-AC 7260 for Desktop
- » Intel® Dual Band Wireless-AC 3160
- » Intel® Wireless-N 7260
- » Broadcom BCM43228\*
- » Broadcom BCM43241\*
- » Broadcom BCM4352\*

#### Operating System:

- » Windows 7 64-bit, Home Premium, Ultimate or Professional
- » Windows 7 32-bit, Home Premium, Ultimate, Professional or Basic
- » Windows 8 32-bit and 64-bit editions
- » Windows 8.1 32-bit and 64-bit editions

#### Software:

- » [Intel® Wireless Display pre-installed and enabled](#)

An Intel® WiDi compatible streaming target such as:

- » WiDi Adapter (e.g. Belkin ScreenCast, D-Link DHD-131, NETGEAR Push2TV ...)
- » HDTV's with built in WiDi Support (e.g. LG Smart TV ...)
- » Any other WiDi compatible CE Devices (e.g. Netgear Media Player NTV200S ...)

More information about Intel® Wireless Display Technology are available on [www.intel.com](http://www.intel.com)

## 4.20 Intel® vPro™ technology

Kontron and Intel® are addressing the security and manageability challenges facing embedded systems today with the implementation of Intel® vPro™ technology to enable: » System integrity » Secure isolation » Remote systems management

First, system integrity is the ability to identify whether the system hardware or system software has been modified without authorization. When a system's integrity is known, the system can be thought of as a trusted system. Second, secure isolation is the ability to use platform hardware to separate processes, resources, and data on the system such that they cannot interact with each other in unintended ways. By providing hardware-assisted isolation, there is limitless security, privacy, and cost savings that can be realized through consolidation and workload isolation. Finally, remote systems management is the ability to troubleshoot, perform power management or system verification through secure channels. Significant cost savings and efficiencies can be realized through remote management allowing for increased system up time and the ability to manage or diagnose a system, even when powered down.

Intel® vPro™ technology itself is special functionality designed into both, the processor and the chipset. The three technologies that comprise Intel® vPro™ technology are: Intel Virtualization Technology (Intel® VT), Intel Trusted Execution Technology (Intel® TXT) and Intel Active Management Technology (Intel® AMT).

Intel® VT provides hardware-based assists making secure isolation more efficient and decreases the virtualization footprint, lowering the effective attack surface of a solution. This hardware-based technology can help to protect applications and information by running multiple operating systems (OSs) in isolation on the same physical system. A virtual guest OS can be created in an entirely separate space on the physical system to run specialized or critical



applications. Virtual environments leverage Intel® VT for memory, CPU, and Directed I/O virtualization. Intel® TXT provides the ability to use hardware-based mechanisms to verify system integrity during the boot process. It also provides system memory scrubbing that protects against soft reset attacks. Virtualized environments take advantage of Intel® TXT launch environment verification to establish a dynamic root of trust providing added security to hypervisor or virtual machine monitor (VMM).

Mechanisms employed by Intel® AMT include domain authentication, session keys, persistent data storage in the Intel® AMT hardware, and access control lists. Only firmware images that are digitally signed by Intel are permitted to load and execute. This set of hardware-based features is targeted for businesses and allows remote access to the system, whether wired or wireless, for management and security tasks. Because of the special hardware capabilities provided by Intel® AMT, out of band access is available even when the OS is not functional or system power is off.



Intel® TXT and Intel® AMT are disabled by default. Please contact your local sales or support for BIOS versions with full vPro™ support

## 4.21 ACPI Suspend Modes and Resume Events

The COMe-bHL6 supports the S-states S0, S3, S4, S5. S5eco Support: YES

### The following events resume the system from S3:

- » USB Keyboard (1)
- » USB Mouse (1)
- » Power Button
- » WakeOnLan (2)

### The following events resume the system from S4:

- » Power Button
- » WakeOnLan (2)

### The following events resume the system from S5:

- » Power Button
- » WakeOnLan (2)

### The following events resume the system from S5Eco:

- » Power Button



- (1) OS must support wake up via USB devices and baseboard must power the USB Port with StBy-Voltage
- (2) Depending on the Used Ethernet MAC/Phy WakeOnLan must be enabled in BIOS setup and driver options

## 5 System Resources

### 5.1 Interrupt Request (IRQ) Lines

| IRQ # | Used For   | Available | Comment   |
|-------|------------|-----------|---|
| 0     | Timer0     | No        | -   |
| 1     | Keyboard   | No        | -   |
| 2     | Cascade    | No        | -   |
| 3     | COM2       | No        | onboard UART2   |
| 4     | COM1       | No        | onboard UART1   |
| 5     | SIO LPT    | Note(4)   | external SIO LPT  |
| 6     | COM3       | Note(4)   | external SIO COM1   |
| 7     | COM4       | Note(4)   | external SIO COM2   |
| 8     | RTC        | No        | -   |
| 9     | ACPI       | No        | -   |
| 10    | -          | Yes       | -   |
| 11    | -          | Yes       | -   |
| 12    | PS/2 Mouse | Note(4)   | external SIO  |
| 13    | FPU        | No        | -   |
| 14    | -          | Yes       | -   |
| 15    | -          | Yes       | -   |
| 16    | LNK A      | No        | P.E.G + I.G.D + SA Audio + XHCI + Intel ME + USB EHCI2 + PCIe RP 0 + PCIe RP 4; Note(3) |
| 17    | LNK B      | No        | PCIe RP 1 + PCIe RP 5; Note(3)  |
| 18    | LNK C      | No        | PCIe RP 2 + PCIe RP 6 + SMBus; Note(3)  |
| 19    | LNK D      | No        | PCIe RP 3 + SATA; Note(3)   |
| 20    | LNK E      | No        | Onboard LAN;Note(3)   |
| 21    | LNK F      | No        | Note(3)   |
| 22    | LNK G      | No        | PCH HDA;Note(3)   |
| 23    | LNK H      | No        | USB EHCI#1  |

(1) If the "Used For" device is disabled in setup, the corresponding interrupt is available for other device.



(2) Not available if ACPI is used

(3) ACPI OS decides on particular IRQ usage

(4) Depends on system configuration (onboard COM Port support and external SIO presence)

## 5.2 Memory Area

The first 640 kB of DRAM are used as main memory. Using DOS, you can address 1 MB of memory directly. Memory area above 1 MB (high memory, extended memory) is accessed under DOS via special drivers such as HIMEM.SYS and EMM386.EXE, which are part of the operating system. Please refer to the operating system documentation or special textbooks for information about HIMEM.SYS and EMM386.EXE. Other operating systems (Linux or Windows versions) allow you to address the full memory area directly.

| Upper Memory         | Used for             | Available | Comment   |
|----------------------|----------------------|-----------|---|
| A0000h – BFFFFh      | VGA Memory           | No        | Mainly used by graphic controller               |
| C0000h – CFFFFh      | VGA BIOS             | No        | Used by onboard VGA ROM                         |
| D0000h – DFFFFh      | -                    | Yes       | Free for shadow RAM in standard configurations. |
| E0000h – FFFFFh      | System BIOS          | No        | Fixed   |
| 20000000h-201FFFFFFh | IGFX                 | No        | Fixed   |
| 40000000h-401FFFFFFh | IGFX                 | No        | Fixed   |
| E0000000h-FEAFFFFFFh | PCIe Config Space    | No        | Fixed   |
| FEC00000 - FECFFFFFF | Local APIC/IOAPIC(s) | No        | Fixed   |
| FED00000h-FED003FFh  | HPET                 | No        | Fixed   |
| FED10000h-FED17FFFh  | MCH                  | No        | Fixed   |
| FED18000h-FED18FFFh  | DMI                  | No        | Fixed   |
| FED19000h-FED19FFFh  | EPBA                 | No        | Fixed   |
| FED1C000h-FED1FFFFh  | RCBA                 | No        | Fixed   |
| FED20000h FED3FFFFh  | TXT                  | No        | Fixed   |
| FED40000h FED44FFFh  | TPM                  | No        | Fixed   |
| FED45000h FED8FFFFh  | TPM                  | No        | Fixed   |
| FED90000h-FED93FFFh  | VT-d                 | No        | Fixed   |
| FEE00000h-FEEFFFFFFh | MSI area             | No        | Fixed   |
| FF000000h-FFFFFFFFh  | BIOS Flash           | No        | Fixed   |

## 5.3 I/O Address Map

The I/O-port addresses of the are functionally identical to a standard PC/AT. All addresses not mentioned in this table should be available. We recommend that you do not use I/O addresses below 0100h with additional hardware for compatibility reasons, even if available.

| I/O Address | Used for               | Available | Comment       |
|-------------|------------------------|-----------|---------------|
| 0000 - 001F | System Resources       | No        | Fixed         |
| 0020 - 003F | Interrupt Controller 1 | No        | Fixed         |
| 002E - 002F | Ext. SIO               | No        | Fixed         |
| 0040 - 005F | Timer, Counter         | No        | Fixed         |
| 004E - 004F | TPM                    | No        | Fixed         |
| 0060 - 006F | Keyboard controller    | No        | Fixed         |
| 0070 - 007F | RTC and CMOS Registers | No        | Fixed         |
| 0080        | BIOS Postcode          | No        | Fixed         |
| 0081 - 009F | DMA Controller         | No        | Fixed         |
| 00A0 - 00BF | Interrupt Controller   | No        | Fixed         |
| 00C0 - 00DF | DMA Controller         | No        | Fixed         |
| 00F0 - 00FF | Math Coprocessor       | No        | Fixed         |
| 03B0 - 03DF | VGA                    | No        | Fixed         |
| 0400 - 047F | Chipset                | No        | Fixed         |
| 04D0 - 04D1 | Chipset                | No        | Fixed         |
| 0800 - 087F | Chipset                | No        | Fixed         |
| 0A00 - 0A0F | LPC                    | Yes       | Routed to LPC |
| 0A80 - 0A8F | CPLD                   | No        | Fixed         |
| 0A90 - 0AFF | LPC                    | Yes       | Routed to LPC |
| 0CF8 - 0CFF | Chipset                | No        | Fixed         |

## 5.4 Peripheral Component Interconnect (PCI) Devices

All devices follow the Peripheral Component Interconnect 2.3 (PCI 2.3) respectively the PCI Express Base 1.0a specification. The BIOS and OS control memory and I/O resources. Please see the PCI 2.3 specification for details.

| PCI Device       | B:D:F  | PCI IRQ | Interface | Comment |
|------------------|--------|---------|-----------|---------|
| Host Bridge      | 0:0:0  | None    | internal  | Chipset |
| P.E.G. Root Port | 0:1:0  | LNK A   | internal  | Chipset |
| Video Controller | 0:2:0  | LNK A   | internal  | Chipset |
| SA Audio         | 0:3:0  | LNK A   | internal  | Chipset |
| XHCI             | 0:20:0 | LNK A   | internal  | Chipset |
| ME               | 0:22:0 | LNK A   | internal  | Chipset |
| GbE              | 0:25:0 | LNK E   | internal  | Chipset |
| EHCI2            | 0:26:0 | LNK A   | internal  | Chipset |
| PCH HDA          | 0:27:0 | LNK G   | PCIe      | Chipset |
| PCIe Port 0      | 0:28:0 | LNK A   | internal  | Chipset |
| PCIe Port 0 Slot | -      | A/B/C/D | PCIe      | Port 0  |
| PCIe Port 1      | 0:28:1 | LNK A   | internal  | Chipset |
| PCIe Port 1 Slot | -      | B/C/D/A | PCIe      | Port 1  |
| PCIe Port 2      | 0:28:2 | LNK A   | internal  | Chipset |
| PCIe Port 2 Slot | -      | C/D/A/B | PCIe      | Port 2  |
| PCIe Port 3      | 0:28:3 | LNK A   | internal  | Chipset |
| PCIe Port 3 Slot | -      | D/A/B/A | PCIe      | Port 3  |
| PCIe Port 4      | 0:28:4 | LNK A   | internal  | Chipset |
| PCIe Port 4 Slot | -      | A/B/C/D | PCIe      | Port 4  |
| PCIe Port 5      | 0:28:5 | LNK A   | internal  | Chipset |
| PCIe Port 5 Slot | -      | B/C/D/A | PCIe      | Port 5  |
| PCIe Port 6      | 0:28:6 | LNK A   | internal  | Chipset |
| PCIe Port 6 Slot | -      | C/D/A/B | PCIe      | Port 6  |
| EHCI1            | 0:29:0 | LNK H   | internal  | Chipset |
| LPC Bridge       | 0:31:0 | -       | internal  | Chipset |
| SATA             | 0:31:2 | LNK D   | internal  | Chipset |
| SMBus            | 0:31:3 | LNK C   | internal  | Chipset |

## 5.5 Internal I2C Bus

| I2C Address | Used For    | Available | Comment                            |
|-------------|-------------|-----------|------------------------------------|
| 58h         | S5 Eco      | No        | S5 Eco Resistor                    |
| A0h         | JILI-EEPROM | No        | external LVDS EEPROM for JILI Data |
| C0h         | LVDS bridge | No        | DP to LVDS Bridge                  |

## 5.6 External I2C Bus

| I2C Address | Used For    | Available | Comment                          |
|-------------|-------------|-----------|----------------------------------|
| A0h         | JIDA-EEPROM | No        | Module EEPROM                    |
| AEh         | FRU-EEPROM  | No        | Recommended for Baseboard EEPROM |

## 5.7 System Management (SM) Bus

The 8-bit SMBus addresses uses the LSB (Bit 0) for the direction. Bit0 = 0 defines the write address, Bit0 = 1 defines the read address for the device. The 8-bit addresses listed below shows the write address for all devices. 7-bit SMBus addresses shows the device address without Bit0.

| 8-bit Address | 7-bit Address | Device                      | Comment  | SMBus |
|---------------|---------------|-----------------------------|--|-------|
| 12h           | 0x09          | SMART_CHARGER               | Not to be used with any SM bus device except a charger             | SMB   |
| 14h           | 0x0A          | SMART_SELECTOR              | Not to be used with any SM bus device except a selector or manager | SMB   |
| 16h           | 0x0B          | SMART_BATTERY               | Not to be used with any SM bus device except a battery             | SMB   |
| 30h           | 0x18          | DDR3 Thermal Sensor Chan. A | Do not use under any circumstances                                 | SMB   |
| 34h           | 0x1A          | DDR3 Thermal Sensor Chan. B | Do not use under any circumstances                                 | SMB   |
| 58h           | 0x2C          | Hardware Monitor            | Do not use under any circumstances                                 | SMB   |
| A0h           | 0x50          | DDR3 channel A SPD          | Do not use under any circumstances                                 | SMB   |
| A4h           | 0x52          | DDR3 channel B SPD          | Do not use under any circumstances                                 | SMB   |
| C8h           | 0x64          | Ethernet I218-LM            | Do not use under any circumstances                                 | SML0  |

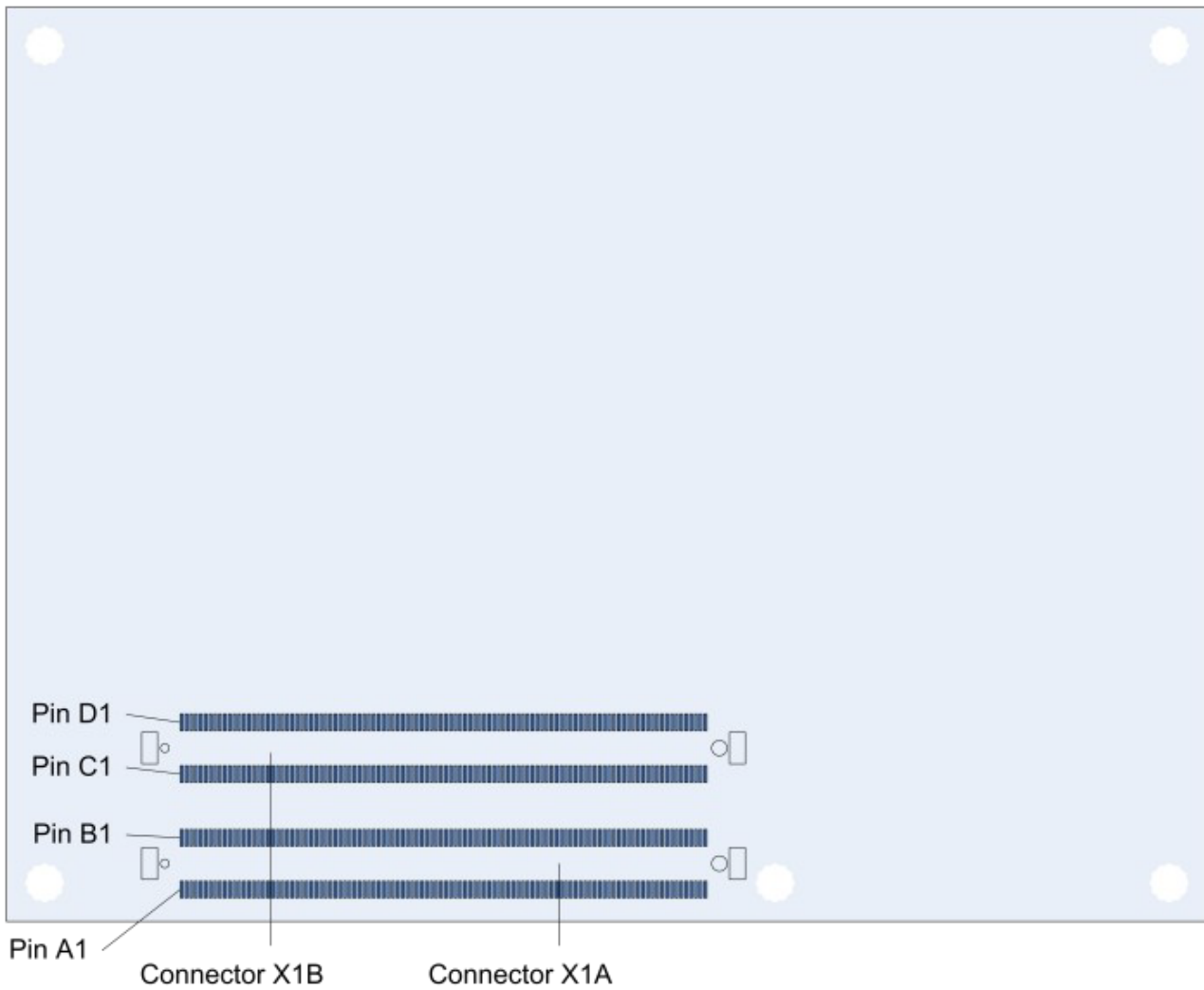


A JIDA Bus No. like in former Modules cannot be provided because the EAPI driver implementation enumerates the I2C busses dynamically. Please follow the initialization process like it is provided in the EAPI specification.

## 6 Connectors

The pin-outs for Interface Connectors X1A and X1B are documented for convenient reference. Please see the COM Express® Specification and COM Express® Design Guide for detailed, design-level information.

### 6.1 Connector Location



## 7 Pinout List

### 7.1 General Signal Description

| Type    | Description                            |
|---------|--|
| I/O-3,3 | Bi-directional 3,3 V I/O-Signal        |
| I/O-5T  | Bi-dir. 3,3V I/O (5V Tolerance)        |
| I/O-5   | Bi-directional 5V I/O-Signal           |
| I-3,3   | 3,3V Input                             |
| I/OD    | Bi-directional Input/Output Open Drain |
| I-5T    | 3,3V Input (5V Tolerance)              |
| OA      | Output Analog                          |
| OD      | Output Open Drain                      |
| O-1,8   | 1,8V Output                            |
| O-3,3   | 3,3V Output                            |
| O-5     | 5V Output                              |
| DP-I/O  | Differential Pair Input/Output         |
| DP-I    | Differential Pair Input                |
| DP-O    | Differential Pair Output               |
| PU      | Pull-Up Resistor                       |
| PD      | Pull-Down Resistor                     |
| PWR     | Power Connection                       |



To protect external power lines of peripheral devices, make sure that: the wires have the right diameter to withstand the maximum available current the enclosure of the peripheral device fulfills the fire-protection requirements of IEC/EN60950

## 7.2 Connector X1A Row A

| Pin | Signal         | Description                              | Type     | Termination       | Comment   |
|-----|----------------|--|----------|-------------------|---|
| A1  | GND            | Power Ground                             | PWR GND  | -                 | -   |
| A2  | GBEO_MDI3-     | Ethernet Media Dependent Interface 3 -   | DP-I/O   | -                 | -   |
| A3  | GBEO_MDI3+     | Ethernet Media Dependent Interface 3 +   | DP-I/O   | -                 | -   |
| A4  | GBEO_LINK100#  | Ethernet 100 Mbit Link Indicator         | OD       | -                 | -   |
| A5  | GBEO_LINK1000# | Ethernet 1000 Mbit Link Indicator        | OD       | -                 | -   |
| A6  | GBEO_MDI2-     | Ethernet Media Dependent Interface 2 -   | DP-I/O   | -                 | -   |
| A7  | GBEO_MDI2+     | Ethernet Media Dependent Interface 2 +   | DP-I/O   | -                 | -   |
| A8  | GBEO_LINK#     | Ethernet Link Indicator                  | OD       | -                 | -   |
| A9  | GBEO_MDI1-     | Ethernet Media Dependent Interface 1 -   | DP-I/O   | -                 | -   |
| A10 | GBEO_MDI1+     | Ethernet Media Dependent Interface 1 +   | DP-I/O   | -                 | -   |
| A11 | GND            | Power Ground                             | PWR GND  | -                 | -   |
| A12 | GBEO_MDI0-     | Ethernet Media Dependent Interface 0 -   | DP-I/O   | -                 | -   |
| A13 | GBEO_MDI0+     | Ethernet Media Dependent Interface 0 +   | DP-I/O   | -                 | -   |
| A14 | GBEO_CTREF     | Center Tab Reference Voltage             | 0        | -                 | 1µF capacitor to GND  |
| A15 | SUS_S3#        | Suspend To RAM (or deeper) Indicator     | 0-3.3    | PD 10k            | -   |
| A16 | SATA0_TX+      | SATA 0 Transmit Pair +                   | DP-0     | -                 | -   |
| A17 | SATA0_TX-      | SATA 0 Transmit Pair -                   | DP-0     | -                 | -   |
| A18 | SUS_S4#        | Suspend To Disk (or deeper) Indicator    | 0-3.3    | -                 | -   |
| A19 | SATA0_RX+      | SATA 0 Receive Pair +                    | DP-I     | -                 | -   |
| A20 | SATA0_RX-      | SATA 0 Receive Pair -                    | DP-I     | -                 | -   |
| A21 | GND            | Power Ground                             | PWR GND  | -                 | -   |
| A22 | SATA2_TX+      | SATA 2 Transmit Pair +                   | DP-0     | -                 | -   |
| A23 | SATA2_TX-      | SATA 2 Transmit Pair -                   | DP-0     | -                 | -   |
| A24 | SUS_S5#        | Soft Off Indicator                       | 0-3.3    | -                 | -   |
| A25 | SATA2_RX+      | SATA 2 Receive Pair +                    | DP-I     | -                 | -   |
| A26 | SATA2_RX-      | SATA 2 Receive Pair -                    | DP-I     | -                 | -   |
| A27 | BATLOW#        | Battery Low                              | I-3.3    | PU 10k 3.3V (S5)  | assertion will prevent wake from S3-S5 state  |
| A28 | (S)ATA_ACT#    | Serial ATA LED                           | OD-3.3   | PU 10k 3.3V (S0)  | can pull down 3mA   |
| A29 | AC/HDA_SYnc    | HD Audio Sync                            | 0-3.3    | PD 15k in PCH     | resistor value can range from 9k0hm to 50k0hm   |
| A30 | AC/HDA_RST#    | HD Audio Reset                           | 0-3.3    | -                 | -   |
| A31 | GND            | Power Ground                             | PWR GND  | -                 | -   |
| A32 | AC/HDA_BITCLK  | HD Audio Bit Clock Output                | 0-3.3    | -                 | -   |
| A33 | AC/HDA_SDOUT   | HD Audio Serial Data Out                 | 0-3.3    | PD 15k in PCH     | resistor value can range from 9k0hm to 50k0hm   |
| A34 | BIOS_DIS0#     | BIOS Selection Strap 0                   | I-3.3    | PU 10k 3.3V (SPI) | PU might be powered during suspend  |
| A35 | THRMTRIP#      | Thermal Trip                             | 0-3.3    | PU 10k 3.3V (S0)  | do not use for overtemperatur detection (because this signal is a S0 signal, it's not possible to see if module shuts down regular or caused by CPU overtemperatur) |
| A36 | USB6-          | USB 2.0 Data Pair Port 6 -               | DP-I/O   | PD 15k in PCH     | resistor value can range from 14k0hm to 25k0hm  |
| A37 | USB6+          | USB 2.0 Data Pair Port 6 +               | DP-I/O   | PD 15k in PCH     | resistor value can range from 14k0hm to 25k0hm  |
| A38 | USB_6_7_OC#    | USB Overcurrent Indicator Port 6/7       | I-3.3    | PU 10k 3.3V (S5)  | -   |
| A39 | USB4-          | USB 2.0 Data Pair Port 4 -               | DP-I/O   | PD 15k in PCH     | resistor value can range from 14k0hm to 25k0hm  |
| A40 | USB4+          | USB 2.0 Data Pair Port 4 +               | DP-I/O   | PD 15k in PCH     | resistor value can range from 14k0hm to 25k0hm  |
| A41 | GND            | Power Ground                             | PWR GND  | -                 | -   |
| A42 | USB2-          | USB 2.0 Data Pair Port 2 -               | DP-I/O   | PD 15k in PCH     | resistor value can range from 14k0hm to 25k0hm  |
| A43 | USB2+          | USB 2.0 Data Pair Port 2 +               | DP-I/O   | PD 15k in PCH     | resistor value can range from 14k0hm to 25k0hm  |
| A44 | USB_2_3_OC#    | USB Overcurrent Indicator Port 2/3       | I-3.3    | PU 10k 3.3V (S5)  | -   |
| A45 | USB0-          | USB 2.0 Data Pair Port 0 -               | DP-I/O   | PD 15k in PCH     | resistor value can range from 14k0hm to 25k0hm  |
| A46 | USB0+          | USB 2.0 Data Pair Port 0 +               | DP-I/O   | PD 15k in PCH     | resistor value can range from 14k0hm to 25k0hm  |
| A47 | VCC_RTC        | Real-Time Clock Circuit Power Input      | PWR 3V   | -                 | -   |
| A48 | EXCDO_PERST#   | Express Card Reset Port 0                | 0-3.3    | -                 | -   |
| A49 | EXCDO_CPPE#    | Express Card Capable Card Request Port 0 | I-3.3    | PU 10k 3.3V (S0)  | -   |
| A50 | LPC_SERIRQ     | Serial Interrupt Request                 | I/OD-3.3 | PU 8k25 3.3V (S0) | -   |
| A51 | GND            | Power Ground                             | PWR GND  | -                 | -   |
| A52 | PCIE_TX5+      | PCI Express Lane 5 Transmit +            | DP-0     | -                 | -   |
| A53 | PCIE_TX5-      | PCI Express Lane 5 Transmit -            | DP-0     | -                 | -   |
| A54 | GPIO           | General Purpose Input 0                  | I-3.3    | PU 10k 3.3V (S0)  | -   |
| A55 | PCIE_TX4+      | PCI Express Lane 4 Transmit +            | DP-0     | -                 | -   |
| A56 | PCIE_TX4-      | PCI Express Lane 4 Transmit -            | DP-0     | -                 | -   |
| A57 | GND            | Power Ground                             | PWR GND  | -                 | -   |
| A58 | PCIE_TX3+      | PCI Express Lane 3 Transmit +            | DP-0     | -                 | -   |
| A59 | PCIE_TX3-      | PCI Express Lane 3 Transmit -            | DP-0     | -                 | -   |
| A60 | GND            | Power Ground                             | PWR GND  | -                 | -   |
| A61 | PCIE_TX2+      | PCI Express Lane 2 Transmit +            | DP-0     | -                 | -   |
| A62 | PCIE_TX2-      | PCI Express Lane 2 Transmit -            | DP-0     | -                 | -   |



|      |               |  |             |                     |   |
|------|---------------|--|-------------|---------------------|---|
| A63  | GPI1          | General Purpose Input 1                      | I-3.3       | PU 10k 3.3V (S0)    | -   |
| A64  | PCIE_TX1+     | PCI Express Lane 1 Transmit +                | DP-0        | -                   | -   |
| A65  | PCIE_TX1-     | PCI Express Lane 1 Transmit -                | DP-0        | -                   | -   |
| A66  | GND           | Power Ground                                 | PWR GND     | -                   | -   |
| A67  | GPI2          | General Purpose Input 2                      | I-3.3       | PU 10k 3.3V (S0)    | -   |
| A68  | PCIE_TX0+     | PCI Express Lane 0 Transmit +                | DP-0        | -                   | -   |
| A69  | PCIE_TX0-     | PCI Express Lane 0 Transmit -                | DP-0        | -                   | -   |
| A70  | GND           | Power Ground                                 | PWR GND     | -                   | -   |
| A71  | LVDS_A0+      | LVDS Channel A Data0 +                       | DP-0        | -                   | -   |
| A72  | LVDS_A0-      | LVDS Channel A Data0 -                       | DP-0        | -                   | -   |
| A73  | LVDS_A1+      | LVDS Channel A Data1 +                       | DP-0        | -                   | configuration as eDP_TX1+ in customised article version possible                              |
| A74  | LVDS_A1-      | LVDS Channel A Data1 -                       | DP-0        | -                   | configuration as eDP_TX1- in customised article version possible                              |
| A75  | LVDS_A2+      | LVDS Channel A Data2 +                       | DP-0        | -                   | configuration as eDP_TX0+ in customised article version possible                              |
| A76  | LVDS_A2-      | LVDS Channel A Data2 -                       | DP-0        | -                   | configuration as eDP_TX0- in customised article version possible                              |
| A77  | LVDS_VDD_EN   | LVDS Panel Power Control                     | 0-3.3       | PD 100k             | configuration as eDP_VDD_EN in customised article version possible                            |
| A78  | LVDS_A3+      | LVDS Channel A Data3 +                       | DP-0        | -                   | -   |
| A79  | LVDS_A3-      | LVDS Channel A Data3 -                       | DP-0        | -                   | -   |
| A80  | GND           | Power Ground                                 | PWR GND     | -                   | -   |
| A81  | LVDS_A_CLK+   | LVDS Channel A Clock +                       | DP-0        | -                   | -   |
| A82  | LVDS_A_CLK-   | LVDS Channel A Clock -                       | DP-0        | -                   | -   |
| A83  | LVDS_I2C_CLK  | LVDS Data Channel Clock                      | I/0-3.3     | PU 2k21 3.3V (S0)   | configuration as eDP_AUX+ in customised article version possible                              |
| A84  | LVDS_I2C_DAT  | LVDS Data Channel Data                       | I/0-3.3     | PU 2k21 3.3V (S0)   | configuration as eDP_AUX- in customised article version possible                              |
| A85  | GPI3          | General Purpose Input 3                      | I-3.3       | PU 10k 3.3V (S0)    | -   |
| A86  | RSVD          | Reserved for future use                      | nc          | -                   | -   |
| A87  | RSVD          | Reserved for future use                      | nc          | -                   | configuration as eDP_HPD in customised article version possible                               |
| A88  | PCIE_CLK_REF+ | Reference PCI Express Clock +                | DP-0        | -                   | -   |
| A89  | PCIE_CLK_REF- | Reference PCI Express Clock -                | DP-0        | -                   | -   |
| A90  | GND           | Power Ground                                 | PWR GND     | -                   | -   |
| A91  | SPI_POWER     | 3.3V Power Output Pin for external SPI flash | 0-3.3       | -                   | might be powered during suspend   |
| A92  | SPI_MISO      | SPI Master IN Slave OUT                      | I-3.3       | PU 20k in PCH (SPI) | resistor value can range from 15k0hm to 40k0hm and might be powered during suspend            |
| A93  | GPO0          | General Purpose Output 0                     | 0-3.3       | PD 10k              | -   |
| A94  | SPI_CLK       | SPI Clock                                    | 0-3.3       | -                   | -   |
| A95  | SPI_MOSI      | SPI Master Out Slave In                      | 0-3.3       | PD 20k in PCH       | resistor value can range from 15k0hm to 40k0hm  |
| A96  | TPM_PP        | TPM Physical Presence                        | I-3.3       | PD 100k             | -   |
| A97  | TYPE10#       | No Connect for type 6 modules                | nc          | -                   | -   |
| A98  | SERO_TX       | Serial Port 0 TXD                            | 0-3.3       | -                   | 20V protection circuit implemented on module, PD on carrier board needed for proper operation |
| A99  | SERO_RX       | Serial Port 0 RXD                            | I-5T        | PU 47k 3.3V (S0)    | 20V protection circuit implemented on module  |
| A100 | GND           | Power Ground                                 | PWR GND     | -                   | -   |
| A101 | SER1_TX       | Serial Port 1 TXD                            | 0-3.3       | -                   | 20V protection circuit implemented on module, PD on carrier board needed for proper operation |
| A102 | SER1_RX       | Serial Port 1 RXD                            | I-5T        | PU 47k 3.3V (S0)    | 20V protection circuit implemented on module  |
| A103 | LID#          | LID Switch Input                             | I-3.3       | PU 47k 3.3V (S5)    | 20V protection circuit implemented on module  |
| A104 | VCC_12V       | Main Input Voltage (8.5-20V)                 | PWR 8.5-20V | -                   | -   |
| A105 | VCC_12V       | Main Input Voltage (8.5-20V)                 | PWR 8.5-20V | -                   | -   |
| A106 | VCC_12V       | Main Input Voltage (8.5-20V)                 | PWR 8.5-20V | -                   | -   |
| A107 | VCC_12V       | Main Input Voltage (8.5-20V)                 | PWR 8.5-20V | -                   | -   |
| A108 | VCC_12V       | Main Input Voltage (8.5-20V)                 | PWR 8.5-20V | -                   | -   |
| A109 | VCC_12V       | Main Input Voltage (8.5-20V)                 | PWR 8.5-20V | -                   | -   |
| A110 | GND           | Power Ground                                 | PWR GND     | -                   | -   |

## 7.3 Connector X1A Row B

| Pin | Signal       | Description                               | Type    | Termination         | Comment  |
|-----|--------------|---|---------|---------------------|--|
| B1  | GND          | Power Ground                              | PWR GND | -                   | -  |
| B2  | GBEO_ACT     | Ethernet Activity LED                     | OD      | -                   | -  |
| B3  | LPC_FRAME#   | LPC Frame Indicator                       | 0-3.3   | -                   | -  |
| B4  | LPC_ADO      | LPC Multiplexed Command, Address & Data 0 | I/O-3.3 | PU 20k in PCH (S0)  | resistor value can range from 15k0hm to 40k0hm                     |
| B5  | LPC_AD1      | LPC Multiplexed Command, Address & Data 1 | I/O-3.3 | PU 20k in PCH (S0)  | resistor value can range from 15k0hm to 40k0hm                     |
| B6  | LPC_AD2      | LPC Multiplexed Command, Address & Data 2 | I/O-3.3 | PU 20k in PCH (S0)  | resistor value can range from 15k0hm to 40k0hm                     |
| B7  | LPC_AD3      | LPC Multiplexed Command, Address & Data 3 | I/O-3.3 | PU 20k in PCH (S0)  | resistor value can range from 15k0hm to 40k0hm                     |
| B8  | LPC_DRQ0#    | LPC Serial DMA/Master Request 0           | I-3.3   | PU 20k in PCH (S0)  | resistor value can range from 15k0hm to 40k0hm                     |
| B9  | LPC_DRQ1#    | LPC Serial DMA/Master Request 1           | I-3.3   | PU 20k in PCH (S0)  | resistor value can range from 15k0hm to 40k0hm                     |
| B10 | LPC_CLK      | 33MHz LPC clock                           | 0-3.3   | -                   | -  |
| B11 | GND          | Power Ground                              | PWR GND | -                   | -  |
| B12 | PWRBTN#      | Power Button                              | I-3.3   | PU 10k 3.3V (S5eco) | -  |
| B13 | SMB_CK       | SMBUS Clock                               | 0-3.3   | PU 3k3 3.3V (S5)    | -  |
| B14 | SMB_DAT      | SMBUS Data                                | I/O-3.3 | PU 3k3 3.3V (S5)    | -  |
| B15 | SMB_ALERT#   | SMBUS Alert                               | I/O-3.3 | PU 10k0 3.3V (S5)   | -  |
| B16 | SATA1_TX+    | SATA 1 Transmit Pair +                    | DP-0    | -                   | -  |
| B17 | SATA1_TX-    | SATA 1 Transmit Pair -                    | DP-0    | -                   | -  |
| B18 | SUS_STAT#    | Suspend Status                            | 0-3.3   | -                   | -  |
| B19 | SATA1_RX+    | SATA 1 Receive Pair +                     | DP-I    | -                   | -  |
| B20 | SATA1_RX-    | SATA 1 Receive Pair -                     | DP-I    | -                   | -  |
| B21 | GND          | Power Ground                              | PWR GND | -                   | -  |
| B22 | SATA3_TX+    | SATA 3 Transmit Pair +                    | DP-0    | -                   | -  |
| B23 | SATA3_TX-    | SATA 3 Transmit Pair -                    | DP-0    | -                   | -  |
| B24 | PWR_OK       | Power OK                                  | I-5T    | PU 511k 3.3V        | pullup voltage depends on ATX or single supply mode / 5V tolerant  |
| B25 | SATA3_RX+    | SATA 3 Receive Pair +                     | DP-I    | -                   | -  |
| B26 | SATA3_RX-    | SATA 3 Receive Pair -                     | DP-I    | -                   | -  |
| B27 | WDT          | Watch Dog Time-Out event                  | 0-3.3   | -                   | -  |
| B28 | AC/HDA_SDIN2 | HD Audio Serial Data In 2                 | I-3.3   | PD 15k in PCH       | resistor value can range from 9k0hm to 50k0hm                      |
| B29 | AC/HDA_SDIN1 | HD Audio Serial Data In 1                 | I-3.3   | PD 15k in PCH       | resistor value can range from 9k0hm to 50k0hm                      |
| B30 | AC/HDA_SDIN0 | HD Audio Serial Data In 0                 | I-3.3   | PD 15k in PCH       | resistor value can range from 9k0hm to 50k0hm                      |
| B31 | GND          | Power Ground                              | PWR GND | -                   | -  |
| B32 | SPKR         | Speaker                                   | 0-3.3   | PD 20k in PCH (S0)  | resistor value can range from 15k0hm to 40k0hm, PCH strap function |
| B33 | I2C_CK       | I2C Clock                                 | 0-3.3   | PU 2k21 3.3V (S5)   | -  |
| B34 | I2C_DAT      | I2C Data                                  | I/O-3.3 | PU 2k21 3.3V (S5)   | -  |
| B35 | THRM#        | Over Temperature Input                    | I-3.3   | PU 10k 3.3V (S0)    | no function implemented  |
| B36 | USB7-        | USB 2.0 Data Pair Port 7 -                | DP-I/O  | PD 15K in PCH       | resistor value can range from 14k0hm to 25k0hm                     |
| B37 | USB7+        | USB 2.0 Data Pair Port 7 +                | DP-I/O  | PD 15K in PCH       | resistor value can range from 14k0hm to 25k0hm                     |
| B38 | USB_4_5_OC#  | USB Overcurrent Indicator Port 4/5        | I-3.3   | PU 10k 3.3V (S5)    | -  |
| B39 | USB5-        | USB 2.0 Data Pair Port 5 -                | DP-I/O  | PD 15K in PCH       | resistor value can range from 14k0hm to 25k0hm                     |
| B40 | USB5+        | USB 2.0 Data Pair Port 5 +                | DP-I/O  | PD 15K in PCH       | resistor value can range from 14k0hm to 25k0hm                     |
| B41 | GND          | Power Ground                              | PWR GND | -                   | -  |
| B42 | USB3-        | USB 2.0 Data Pair Port 3 -                | DP-I/O  | PD 15K in PCH       | resistor value can range from 14k0hm to 25k0hm                     |
| B43 | USB3+        | USB 2.0 Data Pair Port 3 +                | DP-I/O  | PD 15K in PCH       | resistor value can range from 14k0hm to 25k0hm                     |
| B44 | USB_0_1_OC#  | USB Overcurrent Indicator Port 0/1        | I-3.3   | PU 10k 3.3V (S5)    | -  |
| B45 | USB1-        | USB 2.0 Data Pair Port 1 -                | DP-I/O  | PD 15K in PCH       | resistor value can range from 14k0hm to 25k0hm                     |
| B46 | USB1+        | USB 2.0 Data Pair Port 1 +                | DP-I/O  | PD 15K in PCH       | resistor value can range from 14k0hm to 25k0hm                     |
| B47 | EXCD1_PERST# | Express Card Reset Port 1                 | 0-3.3   | -                   | -  |
| B48 | EXCD1_CPPE#  | Express Card Capable Card Request Port 1  | I-3.3   | PU 10k 3.3V (S0)    | -  |
| B49 | SYS_RESET#   | Reset Button Input                        | I-3.3   | PU 10k 3.3V (S5)    | -  |
| B50 | CB_RESET#    | Carrier Board Reset                       | 0-3.3   | -                   | -  |
| B51 | GND          | Power Ground                              | PWR GND | -                   | -  |
| B52 | PCIE_RX5+    | PCI Express Lane 5 Receive +              | DP-I    | -                   | -  |
| B53 | PCIE_RX5-    | PCI Express Lane 5 Receive -              | DP-I    | -                   | -  |
| B54 | GPO1         | General Purpose Output 1                  | 0-3.3   | PD 10k              | -  |
| B55 | PCIE_RX4+    | PCI Express Lane 4 Receive +              | DP-I    | -                   | -  |
| B56 | PCIE_RX4-    | PCI Express Lane 4 Receive -              | DP-I    | -                   | -  |
| B57 | GPO2         | General Purpose Output 2                  | 0-3.3   | PD 10k              | -  |
| B58 | PCIE_RX3+    | PCI Express Lane 3 Receive +              | DP-I    | -                   | -  |
| B59 | PCIE_RX3-    | PCI Express Lane 3 Receive -              | DP-I    | -                   | -  |
| B60 | GND          | Power Ground                              | PWR GND | -                   | -  |
| B61 | PCIE_RX2+    | PCI Express Lane 2 Receive +              | DP-I    | -                   | -  |
| B62 | PCIE_RX2-    | PCI Express Lane 2 Receive -              | DP-I    | -                   | -  |



|      |                |                                |             |                   |   |
|------|----------------|--------------------------------|-------------|-------------------|---|
| B63  | GP03           | General Purpose Output 3       | 0-3.3       | PD 10k            | -   |
| B64  | PCIE_RX1+      | PCI Express Lane 1 Receive +   | DP-I        | -                 | -   |
| B65  | PCIE_RX1-      | PCI Express Lane 1 Receive -   | DP-I        | -                 | -   |
| B66  | WAKE0#         | PCI Express Wake Event         | I-3.3       | PU 10k 3.3V (S5)  | -   |
| B67  | WAKE1#         | General Purpose Wake Event     | I-3.3       | PU 10k 3.3V (S5)  | -   |
| B68  | PCIE_RX0+      | PCI Express Lane 0 Receive +   | DP-I        | -                 | -   |
| B69  | PCIE_RX0-      | PCI Express Lane 0 Receive -   | DP-I        | -                 | -   |
| B70  | GND            | Power Ground                   | PWR GND     | -                 | -   |
| B71  | LVDS_B0+       | LVDS Channel B Data0 +         | DP-0        | -                 | -   |
| B72  | LVDS_B0-       | LVDS Channel B Data0 -         | DP-0        | -                 | -   |
| B73  | LVDS_B1+       | LVDS Channel B Data1 +         | DP-0        | -                 | -   |
| B74  | LVDS_B1-       | LVDS Channel B Data1 -         | DP-0        | -                 | -   |
| B75  | LVDS_B2+       | LVDS Channel B Data2 +         | DP-0        | -                 | -   |
| B76  | LVDS_B2-       | LVDS Channel B Data2 -         | DP-0        | -                 | -   |
| B77  | LVDS_B3+       | LVDS Channel B Data3 +         | DP-0        | -                 | -   |
| B78  | LVDS_B3-       | LVDS Channel B Data3 -         | DP-0        | -                 | -   |
| B79  | LVDS_BKLT_EN   | Panel Backlight On             | 0-3.3       | PD 100k           | configuration as eDP_BKLT_EN in customised article version possible                           |
| B80  | GND            | Power Ground                   | PWR GND     | -                 | -   |
| B81  | LVDS_B_CLK+    | LVDS Channel B Clock +         | DP-0        | -                 | -   |
| B82  | LVDS_B_CLK-    | LVDS Channel B Clock -         | DP-0        | -                 | -   |
| B83  | LVDS_BKLT_CTRL | Backlight Brightness Control   | 0-3.3       | -                 | -   |
| B84  | VCC_5V_SBY     | 5V Standby                     | PWR 5V (S5) | -                 | optional (not necessary in single supply mode)  |
| B85  | VCC_5V_SBY     | 5V Standby                     | PWR 5V (S5) | -                 | optional (not necessary in single supply mode)  |
| B86  | VCC_5V_SBY     | 5V Standby                     | PWR 5V (S5) | -                 | optional (not necessary in single supply mode)  |
| B87  | VCC_5V_SBY     | 5V Standby                     | PWR 5V (S5) | -                 | optional (not necessary in single supply mode)  |
| B88  | BIOS_DIS1#     | BIOS Selection Strap 1         | I-3.3       | PU 10k 3.3V (SPI) | PU might be powered during suspend  |
| B89  | VGA_RED        | Red Analog Video Output        | OA          | PD 150R           | -   |
| B90  | GND            | Power Ground                   | PWR GND     | -                 | -   |
| B91  | VGA_GRN        | Green Analog Video Output      | OA          | PD 150R           | -   |
| B92  | VGA_BLU        | Blue Analog Video Output       | OA          | PD 150R           | -   |
| B93  | VGA_HSYnc      | VGA Horizontal Synchronisation | 0-3.3       | -                 | -   |
| B94  | VGA_VSYnc      | VGA Vertical Synchronisation   | 0-3.3       | -                 | -   |
| B95  | VGA_I2C_CLK    | VGA Data Channel Clock         | I/O-3.3     | PU 1k1 3.3V (S0)  | -   |
| B96  | VGA_I2C_DAT    | VGA Data Channel Data          | I/O-3.3     | PU 1k1 3.3V (S0)  | -   |
| B97  | SPI_CS#        | SPI Chip Select                | 0-3.3       | -                 | -   |
| B98  | RSVD           | Reserved for future use        | nc          | -                 | -   |
| B99  | RSVD           | Reserved for future use        | nc          | -                 | -   |
| B100 | GND            | Power Ground                   | PWR GND     | -                 | -   |
| B101 | FAN_PWMOUT     | Fan PWM Output                 | 0-3.3       | -                 | 20V protection circuit implemented on module, PD on carrier board needed for proper operation |
| B102 | FAN_TACHIN     | Fan Tach Input                 | I-3.3       | PU 47k 3.3V (S0)  | 20V protection circuit implemented on module  |
| B103 | SLEEP#         | Sleep Button Input             | I-3.3       | PU 47k 3.3V (S5)  | 20V protection circuit implemented on module  |
| B104 | VCC_12V        | Main Input Voltage (8.5-20V)   | PWR 8.5-20V | -                 | -   |
| B105 | VCC_12V        | Main Input Voltage (8.5-20V)   | PWR 8.5-20V | -                 | -   |
| B106 | VCC_12V        | Main Input Voltage (8.5-20V)   | PWR 8.5-20V | -                 | -   |
| B107 | VCC_12V        | Main Input Voltage (8.5-20V)   | PWR 8.5-20V | -                 | -   |
| B108 | VCC_12V        | Main Input Voltage (8.5-20V)   | PWR 8.5-20V | -                 | -   |
| B109 | VCC_12V        | Main Input Voltage (8.5-20V)   | PWR 8.5-20V | -                 | -   |
| B110 | GND            | Power Ground                   | PWR GND     | -                 | -   |

## 7.4 Connector X1B Row C

| Pin | Signal             | Description                                    | Type           | Termination  | Comment  |
|-----|--------------------|--|----------------|--------------|--|
| C1  | GND                | Power Ground                                   | PWR GND        | -            | -  |
| C2  | GND                | Power Ground                                   | PWR GND        | -            | -  |
| C3  | USB_SSRX0-         | USB Super Speed Receive Port 0 -               | DP-I           | -            | -  |
| C4  | USB_SSRX0+         | USB Super Speed Receive Port 0 +               | DP-I           | -            | -  |
| C5  | GND                | Power Ground                                   | PWR GND        | -            | -  |
| C6  | USB_SSRX1-         | USB Super Speed Receive Port 1 -               | DP-I           | -            | -  |
| C7  | USB_SSRX1+         | USB Super Speed Receive Port 1 +               | DP-I           | -            | -  |
| C8  | GND                | Power Ground                                   | PWR GND        | -            | -  |
| C9  | USB_SSRX2-         | USB Super Speed Receive Port 2 -               | DP-I           | -            | -  |
| C10 | USB_SSRX2+         | USB Super Speed Receive Port 2 +               | DP-I           | -            | -  |
| C11 | GND                | Power Ground                                   | PWR GND        | -            | -  |
| C12 | USB_SSRX3-         | USB Super Speed Receive Port 3 -               | DP-I           | -            | -  |
| C13 | USB_SSRX3+         | USB Super Speed Receive Port 3 +               | DP-I           | -            | -  |
| C14 | GND                | Power Ground                                   | PWR GND        | -            | -  |
| C15 | DDI1_PAIR6+        | DDI1 Pair 6 +                                  | DP-I           | -            | -  |
| C16 | DDI1_PAIR6-        | DDI1 Pair 6 -                                  | DP-I           | -            | -  |
| C17 | RSVD               | Reserved for future use                        | nc             | -            | -  |
| C18 | RSVD               | Reserved for future use                        | nc             | -            | -  |
| C19 | PCIE_RX6+          | PCI Express Lane 6 Receive +                   | DP-I           | -            | -  |
| C20 | PCIE_RX6-          | PCI Express Lane 6 Receive -                   | DP-I           | -            | -  |
| C21 | GND                | Power Ground                                   | PWR GND        | -            | -  |
| C22 | PCIE_RX7+          | No Connect (opt. PCI Express Lane 7 Receive +) | nc (opt. DP-I) | -            | configuration as PCIE_RX7+ in customised article version without LAN controller possible |
| C23 | PCIE_RX7-          | No Connect (opt. PCI Express Lane 7 Receive -) | nc (opt. DP-I) | -            | configuration as PCIE_RX7- in customised article version without LAN controller possible |
| C24 | DDI1_HPD           | DDI1 Hotplug Detect                            | I-3.3          | PD 100k      | -  |
| C25 | DDI1_PAIR4+        | DDI1 Pair 4 +                                  | DP-I           | -            | -  |
| C26 | DDI1_PAIR4-        | DDI1 Pair 4 -                                  | DP-I           | -            | -  |
| C27 | RSVD               | Reserved for future use                        | nc             | -            | -  |
| C28 | RSVD               | Reserved for future use                        | nc             | -            | -  |
| C29 | DDI1_PAIR5+        | DDI1 Pair 5 +                                  | DP-I           | -            | -  |
| C30 | DDI1_PAIR5-        | DDI1 Pair 5 -                                  | DP-I           | -            | -  |
| C31 | GND                | Power Ground                                   | PWR GND        | -            | -  |
| C32 | DDI2_CTRLCLK_AUX+  | Multiplexed DDI2 Data Channel Clock & AUX +    | I/O-3.3        | PD 100k      | 2k21 PU (S0) when DDI2_DDC_AUX_SEL is high   |
| C33 | DDI2_CTRLDATA_AUX- | Multiplexed DDI2 Data Channel Data & AUX -     | I/O-3.3        | PU 100k (S0) | 2k21 PU (S0) when DDI2_DDC_AUX_SEL is high   |
| C34 | DDI2_DDC_AUX_SEL   | DDI2 DDC/AUX Select                            | I-3.3          | PD 1M        | -  |
| C35 | RSVD               | Reserved for future use                        | nc             | -            | -  |
| C36 | DDI3_CTRLCLK_AUX+  | Multiplexed DDI3 Data Channel Clock & AUX +    | I/O-3.3        | PD 100k      | 2k21 PU (S0) when DDI3_DDC_AUX_SEL is high   |
| C37 | DDI3_CTRLDATA_AUX- | Multiplexed DDI3 Data Channel Data & AUX -     | I/O-3.3        | PU 100k (S0) | 2k21 PU (S0) when DDI3_DDC_AUX_SEL is high   |
| C38 | DDI3_DDC_AUX_SEL   | DDI3 DDC/AUX Select                            | I-3.3          | PD 1M        | -  |
| C39 | DDI3_PAIR0+        | DDI3 Pair 0 +                                  | DP-0           | -            | -  |
| C40 | DDI3_PAIR0-        | DDI3 Pair 0 -                                  | DP-0           | -            | -  |
| C41 | GND                | Power Ground                                   | PWR GND        | -            | -  |
| C42 | DDI3_PAIR1+        | DDI3 Pair 1 +                                  | DP-0           | -            | -  |
| C43 | DDI3_PAIR1-        | DDI3 Pair 1 -                                  | DP-0           | -            | -  |
| C44 | DDI3_HPD           | DDI3 Hotplug Detect                            | I-3.3          | PD 100k      | -  |
| C45 | RSVD               | Reserved for future use                        | nc             | -            | -  |
| C46 | DDI3_PAIR2+        | DDI3 Pair 2 +                                  | DP-0           | -            | -  |
| C47 | DDI3_PAIR2-        | DDI3 Pair 2 -                                  | DP-0           | -            | -  |
| C48 | RSVD               | Reserved for future use                        | nc             | -            | -  |
| C49 | DDI3_PAIR3+        | DDI3 Pair 3 +                                  | DP-0           | -            | -  |
| C50 | DDI3_PAIR3-        | DDI3 Pair 3 -                                  | DP-0           | -            | -  |
| C51 | GND                | Power Ground                                   | PWR GND        | -            | -  |
| C52 | PEG_RX0+           | PCI Express Graphics Lane 0 Receive +          | DP-I           | -            | -  |
| C53 | PEG_RX0-           | PCI Express Graphics Lane 0 Receive -          | DP-I           | -            | -  |
| C54 | TYPE0#             | No Connect for type 6 module                   | nc             | -            | -  |
| C55 | PEG_RX1+           | PCI Express Graphics Lane 1 Receive +          | DP-I           | -            | -  |
| C56 | PEG_RX1-           | PCI Express Graphics Lane 1 Receive -          | DP-I           | -            | -  |
| C57 | TYPE1#             | No Connect for type 6 module                   | nc             | -            | -  |
| C58 | PEG_RX2+           | PCI Express Graphics Lane 2 Receive +          | DP-I           | -            | -  |
| C59 | PEG_RX2-           | PCI Express Graphics Lane 2 Receive -          | DP-I           | -            | -  |
| C60 | GND                | Power Ground                                   | PWR GND        | -            | -  |
| C61 | PEG_RX3+           | PCI Express Graphics Lane 3 Receive +          | DP-I           | -            | -  |
| C62 | PEG_RX3-           | PCI Express Graphics Lane 3 Receive -          | DP-I           | -            | -  |

|      |           |  |             |   |   |
|------|-----------|--|-------------|---|---|
| C63  | RSVD      | Reserved for future use                | nc          | - | - |
| C64  | RSVD      | Reserved for future use                | nc          | - | - |
| C65  | PEG_RX4+  | PCI Express Graphics Lane 4 Receive +  | DP-I        | - | - |
| C66  | PEG_RX4-  | PCI Express Graphics Lane 4 Receive -  | DP-I        | - | - |
| C67  | RSVD      | Reserved for future use                | nc          | - | - |
| C68  | PEG_RX5+  | PCI Express Graphics Lane 5 Receive +  | DP-I        | - | - |
| C69  | PEG_RX5-  | PCI Express Graphics Lane 5 Receive -  | DP-I        | - | - |
| C70  | GND       | Power Ground                           | PWR GND     | - | - |
| C71  | PEG_RX6+  | PCI Express Graphics Lane 6 Receive +  | DP-I        | - | - |
| C72  | PEG_RX6-  | PCI Express Graphics Lane 6 Receive -  | DP-I        | - | - |
| C73  | GND       | Power Ground                           | PWR GND     | - | - |
| C74  | PEG_RX7+  | PCI Express Graphics Lane 7 Receive +  | DP-I        | - | - |
| C75  | PEG_RX7-  | PCI Express Graphics Lane 7 Receive -  | DP-I        | - | - |
| C76  | GND       | Power Ground                           | PWR GND     | - | - |
| C77  | RSVD      | Reserved for future use                | nc          | - | - |
| C78  | PEG_RX8+  | PCI Express Graphics Lane 8 Receive +  | DP-I        | - | - |
| C79  | PEG_RX8-  | PCI Express Graphics Lane 8 Receive -  | DP-I        | - | - |
| C80  | GND       | Power Ground                           | PWR GND     | - | - |
| C81  | PEG_RX9+  | PCI Express Graphics Lane 9 Receive +  | DP-I        | - | - |
| C82  | PEG_RX9-  | PCI Express Graphics Lane 9 Receive -  | DP-I        | - | - |
| C83  | RSVD      | Reserved for future use                | nc          | - | - |
| C84  | GND       | Power Ground                           | PWR GND     | - | - |
| C85  | PEG_RX10+ | PCI Express Graphics Lane 10 Receive + | DP-I        | - | - |
| C86  | PEG_RX10- | PCI Express Graphics Lane 10 Receive - | DP-I        | - | - |
| C87  | GND       | Power Ground                           | PWR GND     | - | - |
| C88  | PEG_RX11+ | PCI Express Graphics Lane 11 Receive + | DP-I        | - | - |
| C89  | PEG_RX11- | PCI Express Graphics Lane 11 Receive - | DP-I        | - | - |
| C90  | GND       | Power Ground                           | PWR GND     | - | - |
| C91  | PEG_RX12+ | PCI Express Graphics Lane 12 Receive + | DP-I        | - | - |
| C92  | PEG_RX12- | PCI Express Graphics Lane 12 Receive - | DP-I        | - | - |
| C93  | GND       | Power Ground                           | PWR GND     | - | - |
| C94  | PEG_RX13+ | PCI Express Graphics Lane 13 Receive + | DP-I        | - | - |
| C95  | PEG_RX13- | PCI Express Graphics Lane 13 Receive - | DP-I        | - | - |
| C96  | GND       | Power Ground                           | PWR GND     | - | - |
| C97  | RSVD      | Reserved for future use                | nc          | - | - |
| C98  | PEG_RX14+ | PCI Express Graphics Lane 14 Receive + | DP-I        | - | - |
| C99  | PEG_RX14- | PCI Express Graphics Lane 14 Receive - | DP-I        | - | - |
| C100 | GND       | Power Ground                           | PWR GND     | - | - |
| C101 | PEG_RX15+ | PCI Express Graphics Lane 15 Receive + | DP-I        | - | - |
| C102 | PEG_RX15- | PCI Express Graphics Lane 15 Receive - | DP-I        | - | - |
| C103 | GND       | Power Ground                           | PWR GND     | - | - |
| C104 | VCC_12V   | Main Input Voltage (8.5-20V)           | PWR 8.5-20V | - | - |
| C105 | VCC_12V   | Main Input Voltage (8.5-20V)           | PWR 8.5-20V | - | - |
| C106 | VCC_12V   | Main Input Voltage (8.5-20V)           | PWR 8.5-20V | - | - |
| C107 | VCC_12V   | Main Input Voltage (8.5-20V)           | PWR 8.5-20V | - | - |
| C108 | VCC_12V   | Main Input Voltage (8.5-20V)           | PWR 8.5-20V | - | - |
| C109 | VCC_12V   | Main Input Voltage (8.5-20V)           | PWR 8.5-20V | - | - |
| C110 | GND       | Power Ground                           | PWR GND     | - | - |

## 7.5 Connector X1B Row D

| Pin | Signal            | Description                                     | Type           | Termination      | Comment  |
|-----|-------------------|---|----------------|------------------|--|
| D1  | GND               | Power Ground                                    | PWR GND        | -                | -  |
| D2  | GND               | Power Ground                                    | PWR GND        | -                | -  |
| D3  | USB_SSTX0-        | USB Super Speed Transmit Port 0 -               | DP-0           | -                | -  |
| D4  | USB_SSTX0+        | USB Super Speed Transmit Port 0 +               | DP-0           | -                | -  |
| D5  | GND               | Power Ground                                    | PWR GND        | -                | -  |
| D6  | USB_SSTX1-        | USB Super Speed Transmit Port 1 -               | DP-0           | -                | -  |
| D7  | USB_SSTX1+        | USB Super Speed Transmit Port 1 +               | DP-0           | -                | -  |
| D8  | GND               | Power Ground                                    | PWR GND        | -                | -  |
| D9  | USB_SSTX2-        | USB Super Speed Transmit Port 2 -               | DP-0           | -                | -  |
| D10 | USB_SSTX2+        | USB Super Speed Transmit Port 2 +               | DP-0           | -                | -  |
| D11 | GND               | Power Ground                                    | PWR GND        | -                | -  |
| D12 | USB_SSTX3-        | USB Super Speed Transmit Port 3 -               | DP-0           | -                | -  |
| D13 | USB_SSTX3+        | USB Super Speed Transmit Port 3 +               | DP-0           | -                | -  |
| D14 | GND               | Power Ground                                    | PWR GND        | -                | -  |
| D15 | DDI1_CTRLCLK_AUX+ | Multiplexed DDI1 Data Channel Clock & AUX +     | I/O-3.3        | PD 100k          | 2k21 PU (S0) when DDI1_DDC_AUX_SEL is high   |
| D16 | DDI1_CTRLCLK_AUX- | Multiplexed DDI1 Data Channel Data & AUX -      | I/O-3.3        | PU 100k (S0)     | 2k21 PU (S0) when DDI1_DDC_AUX_SEL is high   |
| D17 | RSVD              | Reserved for future use                         | nc             | -                | -  |
| D18 | RSVD              | Reserved for future use                         | nc             | -                | -  |
| D19 | PCIE_TX6+         | PCI Express Lane 6 Transmit +                   | DP-0           | -                | -  |
| D20 | PCIE_TX6-         | PCI Express Lane 6 Transmit -                   | DP-0           | -                | -  |
| D21 | GND               | Power Ground                                    | PWR GND        | -                | -  |
| D22 | PCIE_TX7+         | No Connect (opt. PCI Express Lane 7 Transmit +) | nc (opt. DP-0) | -                | configuration as PCIE_RX7+ in customised article version without LAN controller possible |
| D23 | PCIE_TX7-         | No Connect (opt. PCI Express Lane 7 Transmit -) | nc (opt. DP-0) | -                | configuration as PCIE_RX7- in customised article version without LAN controller possible |
| D24 | RSVD              | Reserved for future use                         | nc             | -                | -  |
| D25 | RSVD              | Reserved for future use                         | nc             | -                | -  |
| D26 | DDI1_PAIR0+       | DDI1 Pair 0 +                                   | DP-0           | -                | -  |
| D27 | DDI1_PAIR0-       | DDI1 Pair 0 -                                   | DP-0           | -                | -  |
| D28 | RSVD              | Reserved for future use                         | nc             | -                | -  |
| D29 | DDI1_PAIR1+       | DDI1 Pair 1 +                                   | DP-0           | -                | -  |
| D30 | DDI1_PAIR1-       | DDI1 Pair 1 -                                   | DP-0           | -                | -  |
| D31 | GND               | Power Ground                                    | PWR GND        | -                | -  |
| D32 | DDI1_PAIR2+       | DDI1 Pair 2 +                                   | DP-0           | -                | -  |
| D33 | DDI1_PAIR2-       | DDI1 Pair 2 -                                   | DP-0           | -                | -  |
| D34 | DDI1_DDC_AUX_SEL  | DDI1 DDC/AUX Select                             | I-3.3          | PD 1M            | -  |
| D35 | RSVD              | Reserved for future use                         | nc             | -                | -  |
| D36 | DDI1_PAIR3+       | DDI1 Pair 3 +                                   | DP-0           | -                | -  |
| D37 | DDI1_PAIR3-       | DDI1 Pair 3 -                                   | DP-0           | -                | -  |
| D38 | RSVD              | Reserved for future use                         | PWR GND        | -                | pin might change to Not Connect (nc) in later product revision                           |
| D39 | DDI2_PAIR0+       | DDI2 Pair 0 +                                   | DP-0           | -                | -  |
| D40 | DDI2_PAIR0-       | DDI2 Pair 0 -                                   | DP-0           | -                | -  |
| D41 | GND               | Power Ground                                    | PWR GND        | -                | -  |
| D42 | DDI2_PAIR1+       | DDI2 Pair 1 +                                   | DP-0           | -                | -  |
| D43 | DDI2_PAIR1-       | DDI2 Pair 1 -                                   | DP-0           | -                | -  |
| D44 | DDI2_HPD          | DDI2 Hotplug Detect                             | I-3.3          | PD 100k          | -  |
| D45 | RSVD              | Reserved for future use                         | nc             | -                | -  |
| D46 | DDI2_PAIR2+       | DDI2 Pair 2 +                                   | DP-0           | -                | -  |
| D47 | DDI2_PAIR2-       | DDI2 Pair 2 -                                   | DP-0           | -                | -  |
| D48 | RSVD              | Reserved for future use                         | nc             | -                | -  |
| D49 | DDI2_PAIR3+       | DDI2 Pair 3 +                                   | DP-0           | -                | -  |
| D50 | DDI2_PAIR3-       | DDI2 Pair 3 -                                   | DP-0           | -                | -  |
| D51 | GND               | Power Ground                                    | PWR GND        | -                | -  |
| D52 | PEG_TX0+          | PCI Express Graphics Lane 0 Transmit +          | DP-0           | -                | -  |
| D53 | PEG_TX0-          | PCI Express Graphics Lane 0 Transmit -          | DP-0           | -                | -  |
| D54 | PEG_Lane_RV#      | PCI Express Graphics Lane Reversal              | I-3.3          | PU 10k 3.3V (S0) | -  |
| D55 | PEG_TX1+          | PCI Express Graphics Lane 1 Transmit +          | DP-0           | -                | -  |
| D56 | PEG_TX1-          | PCI Express Graphics Lane 1 Transmit -          | DP-0           | -                | -  |
| D57 | TYPE2#            | GND for type 6 module                           | O-PWR          | -                | -  |
| D58 | PEG_TX2+          | PCI Express Graphics Lane 2 Transmit +          | DP-0           | -                | -  |
| D59 | PEG_TX2-          | PCI Express Graphics Lane 2 Transmit -          | DP-0           | -                | -  |
| D60 | GND               | Power Ground                                    | PWR GND        | -                | -  |
| D61 | PEG_TX3+          | PCI Express Graphics Lane 3 Transmit +          | DP-0           | -                | -  |
| D62 | PEG_TX3-          | PCI Express Graphics Lane 3 Transmit -          | DP-0           | -                | -  |

|      |           |   |             |   |   |
|------|-----------|---|-------------|---|---|
| D63  | RSVD      | Reserved for future use                 | nc          | - | - |
| D64  | RSVD      | Reserved for future use                 | nc          | - | - |
| D65  | PEG_TX4+  | PCI Express Graphics Lane 4 Transmit +  | DP-0        | - | - |
| D66  | PEG_TX4-  | PCI Express Graphics Lane 4 Transmit -  | DP-0        | - | - |
| D67  | GND       | Power Ground                            | PWR GND     | - | - |
| D68  | PEG_TX5+  | PCI Express Graphics Lane 5 Transmit +  | DP-0        | - | - |
| D69  | PEG_TX5-  | PCI Express Graphics Lane 5 Transmit -  | DP-0        | - | - |
| D70  | GND       | Power Ground                            | PWR GND     | - | - |
| D71  | PEG_TX6+  | PCI Express Graphics Lane 6 Transmit +  | DP-0        | - | - |
| D72  | PEG_TX6-  | PCI Express Graphics Lane 6 Transmit -  | DP-0        | - | - |
| D73  | GND       | Power Ground                            | PWR GND     | - | - |
| D74  | PEG_TX7+  | PCI Express Graphics Lane 7 Transmit +  | DP-0        | - | - |
| D75  | PEG_TX7-  | PCI Express Graphics Lane 7 Transmit -  | DP-0        | - | - |
| D76  | GND       | Power Ground                            | PWR GND     | - | - |
| D77  | RSVD      | Reserved for future use                 | nc          | - | - |
| D78  | PEG_TX8+  | PCI Express Graphics Lane 8 Transmit +  | DP-0        | - | - |
| D79  | PEG_TX8-  | PCI Express Graphics Lane 8 Transmit -  | DP-0        | - | - |
| D80  | GND       | Power Ground                            | PWR GND     | - | - |
| D81  | PEG_TX9+  | PCI Express Graphics Lane 9 Transmit +  | DP-0        | - | - |
| D82  | PEG_TX9-  | PCI Express Graphics Lane 9 Transmit -  | DP-0        | - | - |
| D83  | RSVD      | Reserved for future use                 | nc          | - | - |
| D84  | GND       | Power Ground                            | PWR GND     | - | - |
| D85  | PEG_TX10+ | PCI Express Graphics Lane 10 Transmit + | DP-0        | - | - |
| D86  | PEG_TX10- | PCI Express Graphics Lane 10 Transmit - | DP-0        | - | - |
| D87  | GND       | Power Ground                            | PWR GND     | - | - |
| D88  | PEG_TX11+ | PCI Express Graphics Lane 11 Transmit + | DP-0        | - | - |
| D89  | PEG_TX11- | PCI Express Graphics Lane 11 Transmit - | DP-0        | - | - |
| D90  | GND       | Power Ground                            | PWR GND     | - | - |
| D91  | PEG_TX12+ | PCI Express Graphics Lane 12 Transmit + | DP-0        | - | - |
| D92  | PEG_TX12- | PCI Express Graphics Lane 12 Transmit - | DP-0        | - | - |
| D93  | GND       | Power Ground                            | PWR GND     | - | - |
| D94  | PEG_TX13+ | PCI Express Graphics Lane 13 Transmit + | DP-0        | - | - |
| D95  | PEG_TX13- | PCI Express Graphics Lane 13 Transmit - | DP-0        | - | - |
| D96  | GND       | Power Ground                            | PWR GND     | - | - |
| D97  | RSVD      | Reserved for future use                 | nc          | - | - |
| D98  | PEG_TX14+ | PCI Express Graphics Lane 14 Transmit + | DP-0        | - | - |
| D99  | PEG_TX14- | PCI Express Graphics Lane 14 Transmit - | DP-0        | - | - |
| D100 | GND       | Power Ground                            | PWR GND     | - | - |
| D101 | PEG_TX15+ | PCI Express Graphics Lane 15 Transmit + | DP-0        | - | - |
| D102 | PEG_TX15- | PCI Express Graphics Lane 15 Transmit - | DP-0        | - | - |
| D103 | GND       | Power Ground                            | PWR GND     | - | - |
| D104 | VCC_12V   | Main Input Voltage (8.5-20V)            | PWR 8.5-20V | - | - |
| D105 | VCC_12V   | Main Input Voltage (8.5-20V)            | PWR 8.5-20V | - | - |
| D106 | VCC_12V   | Main Input Voltage (8.5-20V)            | PWR 8.5-20V | - | - |
| D107 | VCC_12V   | Main Input Voltage (8.5-20V)            | PWR 8.5-20V | - | - |
| D108 | VCC_12V   | Main Input Voltage (8.5-20V)            | PWR 8.5-20V | - | - |
| D109 | VCC_12V   | Main Input Voltage (8.5-20V)            | PWR 8.5-20V | - | - |
| D110 | GND       | Power Ground                            | PWR GND     | - | - |



The termination resistors in these tables are already mounted on the module. Refer to the design guide for information about additional termination resistors.



## 8 BIOS Operation

The BIOS (Basic Input and Output System) or UEFI (Unified Extensible Firmware Interface) records hardware parameters of the system in the CMOS on the Computer-on-Module. It's major functions include execution of the POST(Power-On-Self-Test) during system start-up, saving system parameters and loading the operating system. The BIOS includes a BIOS Setup program that allows to modify system configuration settings. The module is equipped with Phoenix SecureCore, which is located in an onboard SPI serial flash memory.

### 8.1 Determining the BIOS Version

To determine the BIOS version currently used on the Computer-on-Modules please check System Information Page inside Setup

### 8.2 BIOS Update

Kontron provides continuous BIOS updates for Computer-on-Modules. The updates are provided for download on <http://emdcustomersection.kontron.com> with detailed change descriptions within the according Product Change Notification (PCN). Please register for EMD Customer Section to get access to BIOS downloads and PCN service.

Modules with BIOS Region/Setup only inside the flash can be updated with AFU utilities (usually 1-3MB BIOS binary file size) directly. Modules with Intel® Management Engine, Ethernet, Flash Descriptor and other options additionally to the BIOS Region (usually 4-16MB BIOS binary file size) requires a different update process with Intel Flash Utility FPT and a wrapper to backup and restore configurations and the MAC address. Therefore it is strongly recommended to use the batch file inside the BIOS download package available on EMD Customer Section.

- » Boot the module to DOS/EFI Shell with access to the BIOS image and Firmware Update Utility provided on EMD Customer Section
- » Execute Flash.bat in DOS or Flash.nsh in EFI Shell



Any modification of the update process may damage your module!

### 8.3 POST Codes

Important POST codes during boot-up

|    |                             |
|----|-----------------------------|
| 8B | Booted to DOS               |
| 68 | Booted to Setup / EFI Shell |
| 00 | Booted to Windows           |

### 8.4 Setup Guide

The Setup Utility changes system behavior by modifying the Firmware configuration. The setup program uses a number of menus to make changes and turn features on or off.

Functional keystrokes in POST:

|             |   |
|-------------|---|
| [F2]        | Enter Setup   |
| [F5]        | Boot Menu   |
| [ESC] + [2] | Enter Setup via Remote Keyboard in Console Redirection Mode |

Functional keystrokes in Setup:

|       |                       |
|-------|-----------------------|
| [F1]  | Help                  |
| [F9]  | Load default settings |
| [F10] | Save and Exit         |

## Menu Bar

The menu bar at the top of the window lists different menus. Use the left/right arrow keys to make a selection.

## Legend Bar

Use the keys listed in the legend bar on the bottom to make your selections or exit the current menu. The table below describes the legend keys and their alternates.

| Key              | Function  |
|------------------|---|
| ← or → Arrow key | Select a menu.                                  |
| ↑ or ↓ Arrow key | Select fields in current menu.                  |
| <Home> or <End>  | Move cursor to top or bottom of current window. |
| <PgUp> or <PgDn> | Move cursor to next or previous page.           |
| +/- or F5/F6     | Change Option                                   |
| <Enter>          | Execute command or select submenu.              |

## Selecting an Item

Use the ↑ or ↓ key to move the cursor to the field you want. Then use the + and – keys to select a value for that field. The Save Value commands in the Exit menu save the values displayed in all the menus.

## Displaying Submenus

Use the ← or → key to move the cursor to the submenu you want. Then press <Enter>. A pointer (▶) marks all submenus.

## Item Specific Help Window

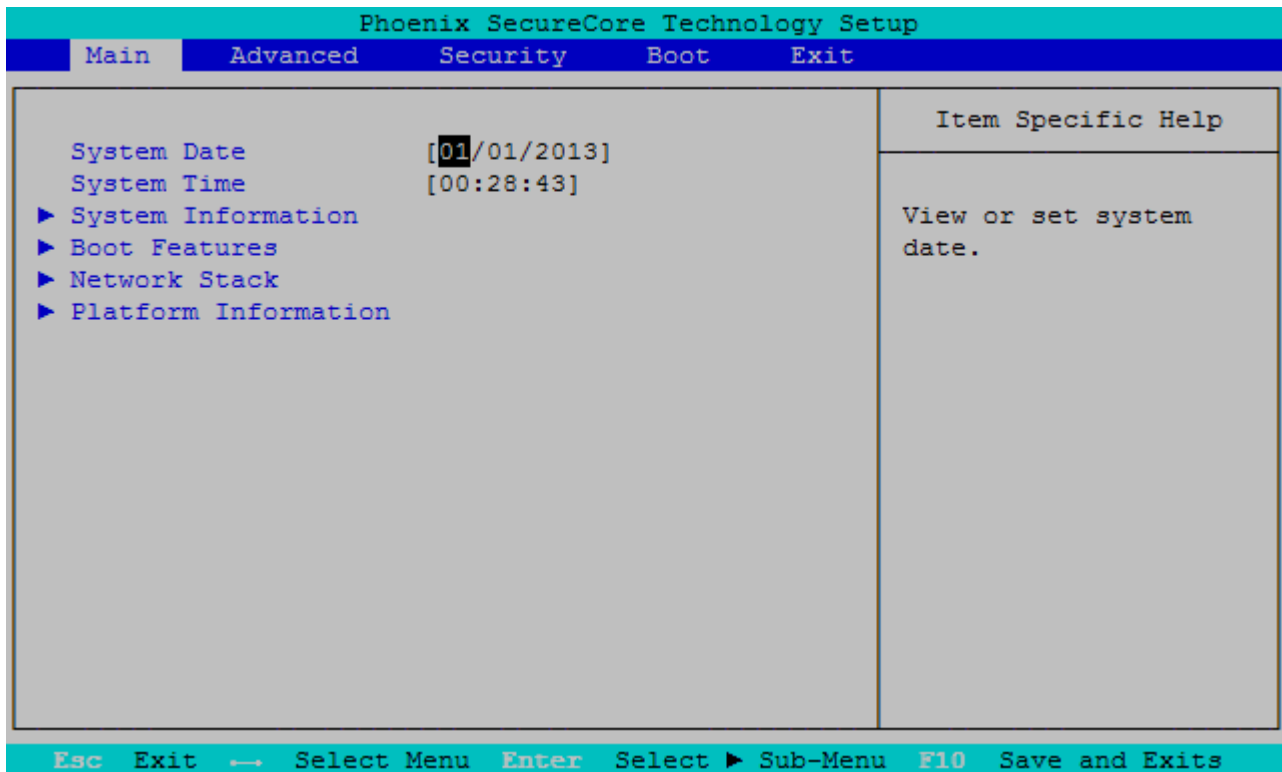
The Help window on the right side of each menu displays the Help text for the selected item. It updates as you move the cursor to each field.

## General Help Window

Pressing <F1> on a menu brings up the General Help window that describes the legend keys and their alternates. Press <Esc> to exit the General Help window.

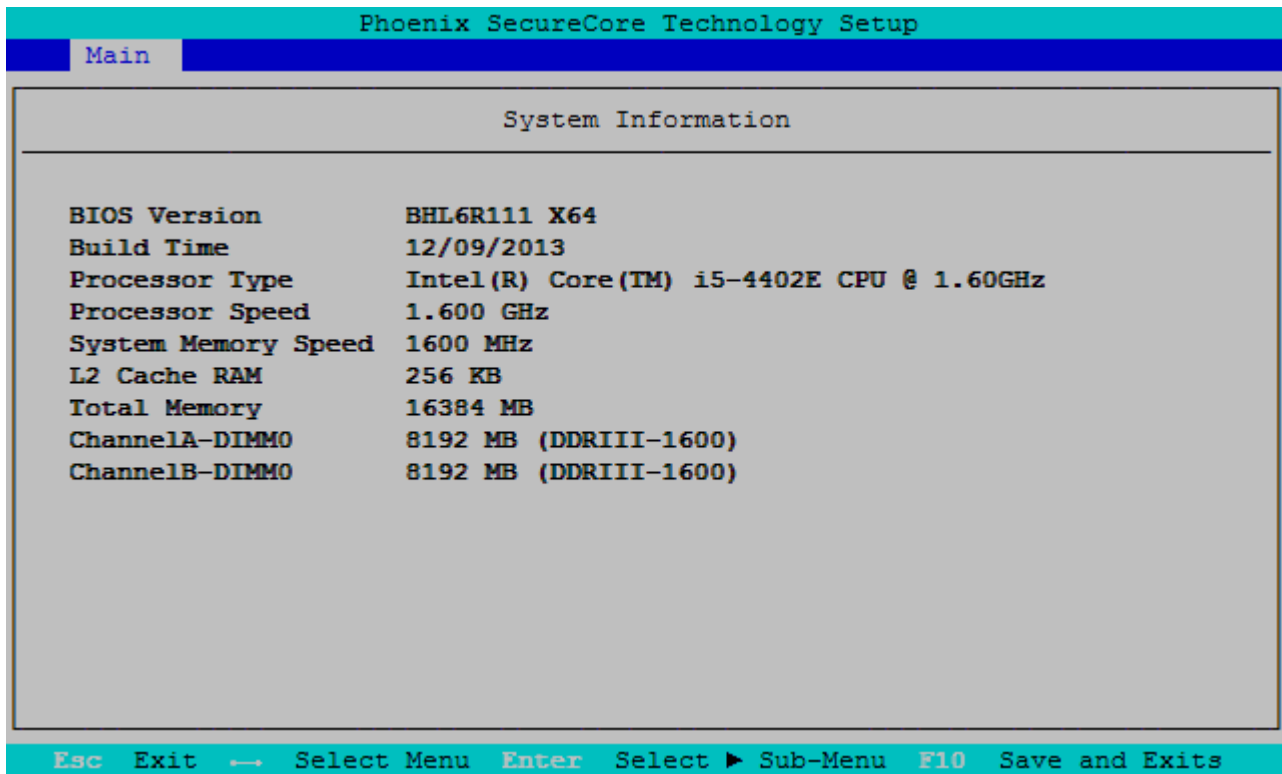
# 8.5 BIOS Setup

## 8.5.1 Main



| Feature     | Options      | Description   |
|-------------|--------------|---|
| System Date | [mm/dd/yyyy] | Set the Date. Use 'Tab' to switch between Date elements |
| System Time | [hh:mm:ss]   | Set the Time. Use 'Tab' to switch between Time elements |


## System Information



## Boot Features

**Phoenix SecureCore Technology Setup**

**Main**

| Boot Features                        | Item Specific Help  |
|--------------------------------------|---|
| NumLock: [On]                        |  |
| Timeout [ 1]                         |   |
| CSM Support [Yes]                    |   |
| Quick Boot [Disabled]                |   |
| Dark Boot [Disabled]                 |   |
| Diagnostic Splash Screen [Disabled]  |   |
| Diagnostic Summary Screen [Disabled] |   |
| BIOS Level USB [Enabled]             |   |
| USB Legacy [Enabled]                 |   |
| Console Redirection [Disabled]       |   |
| Allow Hotkey in S4 resume [Enabled]  |   |
| UEFI Boot [Enabled]                  |   |
| On Shell Exit [Try next]             |   |
| Legacy Boot [Enabled]                |   |
| Boot in Legacy Video Mode [Disabled] |   |
| Load OPROM [On Demand]               |   |
| Boot Priority [UEFI First]           |   |

**Esc** Exit   **←** Select Menu   **Enter** Select   **▶** Sub-Menu   **F10** Save and Exits

| Feature                   | Options  | Description   |
|---------------------------|--|---|
| NumLock                   | <b>On</b><br>Off   | Selects Power-on state for NumLock  |
| Timeout                   | <b>1</b>   | Number of seconds that P.O.S.T will wait for the user input before booting  |
| CSM Support               | <b>Yes</b><br>No   | Enables or Disables the UEFI CSM (Compatibility Support Module) to support legacy PC boot process. Both legacy and UEFI boots are feasible  |
| Quick Boot                | <b>Disabled</b><br>Enabled   | Enable or Disable Quick Boot  |
| Dark Boot                 | <b>Disabled</b><br>Enabled   | Enable or Disable Dark Boot   |
| Diagnostic Splash Screen  | <b>Disabled</b><br>Enabled   | Enable or Disable the Diagnostic Splash Screen  |
| Diagnostic Summary Screen | <b>Disabled</b><br>Enabled   | Display the Diagnostic Summary Screen during boot   |
| BIOS Level USB            | <b>Enabled</b><br>Disabled   | Enable/Disable all BIOS support for USB in order to reduce boot time. Note that this will prevent using a USB keyboard in setup or a USB biometric scanner such as a fingerprint reader to control access to setup, but does not prevent the operating system from supporting such hardware |
| USB Legacy                | <b>Enabled</b><br>Disabled   | Enable/Disable USB BIOS SMM support for mouse, keyboard, mass storage, etc, in legacy operating systems such as DOS   |
| Console Redirection       | <b>Disabled</b><br>Enabled   | Enable/Disable Universal Console Redirection  |
| - Console Port            | All<br><b>Onboard COM1</b><br>Onboard COM2<br>SIO COM1<br>SIO COM2 | Select Port for console redirection. Note: the respective port has to be enabled in setup!  |
| - Terminal Type           | <b>ANSI</b><br>VT100<br>VT100+<br>UTF8                             | Set terminal type of UCR  |
| - Baudrate                | <b>9600</b><br>19200<br>38400<br>57600<br>115200                   | Set terminal type of UCR  |
| - Flow Control            | <b>None</b>  | Set flow control method for UCR. None = No flow   |

|                            |  |   |
|----------------------------|--|---|
|                            | RTS/CTS<br>XON/XOFF                              | control, RTS/CTS = Hardware flow control, XON/XOFF = Software flow control  |
| - Continue C.R. after POST | <b>Enabled</b><br>Disabled                       | Enables Console Redirection after OS has loaded   |
| Allow Hotkey in S4 resume  | <b>Enabled</b><br>Disabled                       | Enable hotkey detection when system resuming from Hibernate state   |
| UEFI Boot                  | <b>Enabled</b><br>Disabled                       | Enable the UEFI boot  |
| On Shell Exit              | <b>Try next</b><br>Launch Setup\Launch Boot Menu | Select behavior after exit from shell   |
| Legacy Boot                | <b>Enabled</b> \Disabled                         | Enable the Legacy boot  |
| Boot in Legacy Video Mode  | <b>Disabled</b><br>Enabled                       | Enable to force the display adapter to switch the video mode to Text Mode 3 at the end of BIOS POST for non-UEFI boot mode (Legacy Boot). Some legacy software, such as DUET, requires that the BIOS explicitly enter text video mode prior to boot |
| Load OPROM                 | <b>On Demand</b><br>All                          | Load all OPROMs or on demand according to the boot device   |
| Boot Priority              | <b>UEFI First</b><br>Legacy First                | Select priority of boot option between UEFI and Legacy  |

## Network Stack

| Phoenix SecureCore Technology Setup |              |                                   |
|-------------------------------------|--------------|-----------------------------------|
| Main                                |              |                                   |
| Network Stack                       |              | Item Specific Help                |
| Network Stack                       | [Enabled]    | Enable/Disable UEFI Network Stack |
| IPv4                                | [Enabled]    |                                   |
| UEFI PXE Boot Priority              | [IPv4 First] |                                   |

Esc Exit → Select Menu Enter Select ► Sub-Menu F10 Save and Exits

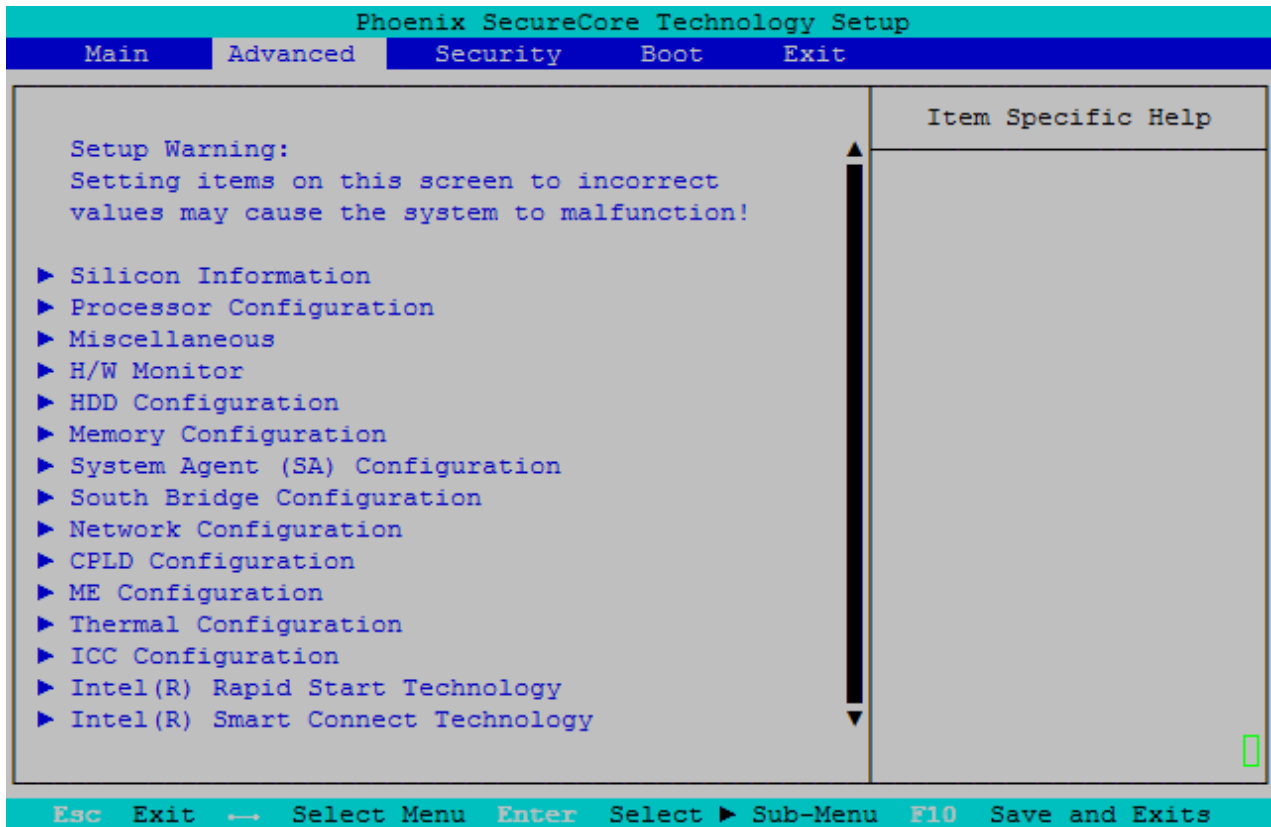
| Feature                | Options             | Description                          |
|------------------------|---------------------|--------------------------------------|
| Network Stack          | Enabled<br>Disabled | Enable / Disable UEFI Network Stack  |
| IPv4                   | Enabled<br>Disabled | Enable / Disable IPv4                |
| UEFI PXE Boot Priority | IPv4 first          | Select PXE Boot Priority (IPv4 only) |

## Platform Information

| Phoenix SecureCore Technology Setup  |                      |
|--|----------------------|
| Main   |                      |
| Platform Information   | Item Specific Help   |
| Module Information<br>Product Name           COMe-bHL6<br>Revision                A.2.4<br>Serial #                 BDD040009<br>MAC Address            00:E0:4B:2C:50:43<br>CPLD Rev               P103.022 (Release)<br>Boot Counter            84 | Platform Information |
| Esc   Exit   ←→   Select Menu   Enter   Select ► Sub-Menu   F10   Save and Exits   |                      |



## 8.5.2 Advanced



## Silicon Information

| Phoenix SecureCore Technology Setup       |                              |
|---|------------------------------|
| Advanced                                  |                              |
| Intel(R) Core(TM) i7-4700EQ CPU @ 2.40GHz |                              |
| FAMILY                                    | 4th Gen Intel Core Processor |
| MODEL                                     | 22nm Haswell Mobile          |
| CPUID                                     | 306C3                        |
| CPU REV.                                  | C1 Stepping                  |
| PATCH ID                                  | 9                            |
| CORE FREQ.                                | 2.40GHz                      |
| L1 Cache                                  | 64 KB                        |
| L2 Cache                                  | 256 KB                       |
| L3 Cache                                  | 8192 KB                      |
| PCH TYPE                                  | LynxPoint                    |
| PCH REV.                                  | C1 Stepping                  |

Esc Exit → Select Menu Enter Select ► Sub-Menu F10 Save and Exits

## Processor Configuration

| Phoenix SecureCore Technology Setup                               |                   |  |
|---|-------------------|--|
| Advanced  |                   |  |
| Processor Configuration   |                   | Item Specific Help                                   |
| Active Processor Cores  | [All]             | Number of cores to enable in each processor package. |
| Intel(R) HT Technology  | [Enabled]         |  |
| CPU Flex Ratio Override   | [Disabled]        |  |
| Enabled XD  | [Enabled]         |  |
| Intel(R) Virtualization Technology                                | [Disabled]        |  |
| <b>Intel(R) Trusted Execution Technol</b>                         | <b>[Disabled]</b> |  |
| ▶ Processor Power Management                                      |                   |  |
| Esc Exit → Select Menu Enter Select ▶ Sub-Menu F10 Save and Exits |                   |  |

| Feature                             | Options                    | Description   |
|-------------------------------------|----------------------------|---|
| Active Processor Cores              | <b>All</b><br>1<br>2<br>3  | Number of cores to enable in each processor package   |
| Intel® HT Technology                | <b>Enabled</b><br>Disabled | When Disabled only one thread per enabled core is enabled   |
| CPU Flex Ratio Override             | <b>Disabled</b><br>Enabled | Enable/Disable CPU Flex Ratio Programming. If Disabled, CPU frequency is set to maximum Ratio automatically   |
| - CPU Flex Ratio Settings           | <b>24</b>                  | This value must be between Max Efficiency Ratio (LFM / Low Frequency Mode) and Maximum non-turbo ratio set by Hardware (High Frequency Mode). See CPU Featureset in chapter Specifications for possible Bus/Core Ratio Settings. The active nominal CPU frequency is Ratio*100MHz |
| Enabled XD                          | <b>Enabled</b><br>Disabled | Enables/Disables 'Execute Disable functionality', also known as Data Execution Prevention DEP   |
| Intel® Virtualization Technology    | <b>Disabled</b><br>Enabled | When enabled, a VMM can utilize the additional hardware capabilities  |
| Intel® Trusted Execution Technology | <b>Disabled</b><br>Enabled | Enable/Disable Intel TXT (enabled only in customized BIOS versions)   |

## Processor Power Management

**Phoenix SecureCore Technology Setup**

**Advanced**

| Processor Power Management              | Item Specific Help |
|---|--------------------|
| Intel(R) SpeedStep(tm) [Enabled]        | ▲<br>↓             |
| Boot Performance Mode [Max Performance] |                    |
| Turbo Mode [Enabled]                    |                    |
| Turbo Mode Power Limit Lock [Disabled]  |                    |
| Long Power Limit [ 0]                   |                    |
| Long Power Limit Time [28]              |                    |
| Short Power Limit [ 0]                  |                    |
| Short Duration Turbo Mode [Enabled]     |                    |
| Energy Efficient Enable [Enabled]       |                    |
| Configure TDP Boot Mode [Nominal]       |                    |
| Lock TDP setting [Disabled]             |                    |
| C-States [Enabled]                      |                    |
| Extend C-States [Enabled]               |                    |
| C3-State [Enabled]                      |                    |
| C6-State [Enabled]                      |                    |
| C6 Latency [Short]                      |                    |
| C7-State [C7s]                          |                    |
| C7 Latency [Long]                       |                    |
| C-State Auto Demotion [C1 and C3]       |                    |
| C-State UnDemotion [C1 and C3]          |                    |
| Package C State Demotion [Disabled]     |                    |
| Package C State UnDemotion [Disabled]   |                    |
| C State Pre-Wake [Enabled]              |                    |

**Esc Exit   ← Select Menu   Enter Select ▶ Sub-Menu   F10 Save and Exits**

| Feature                       | Options                                | Description  |
|-------------------------------|--|--|
| Intel® SpeedStep(TM)          | Enabled<br>Disabled                    | Enable/Disable processor performance states (P-States)   |
| Boot Performance Mode         | Max Performance<br>Max Battery<br>Auto | Select the performance state that the BIOS sets before OS hand-off   |
| Turbo Mode                    | Enabled<br>Disabled                    | Enable processor Turbo Mode  |
| - Turbo Mode Power Limit Lock | Disabled<br>Enabled                    | Enable/Disable Locking of turbo settings. When enabled, Turbo_Power_Limit MSR will be locked and a reset will be required to unlock the register   |
| - Long Power Limit            | 0                                      | Turbo Mode Long Duration Power Limit (also known as Power Limit PL1) in Watts. The value may vary from 0 to Fused Value. If the value is 0, the fused value will be programmed. A value greater than fused TDP value will not be programmed  |
| - Long Power Limit Time       | 28                                     | Long Duration Time Windows (also known as PL1 Time) value in seconds. The value may vary from 0 to 56. Indicates the time window over which TDP value should be maintained. If the value is 0, the fused value will be programmed            |
| - Short Power Limit           | 0                                      | Turbo Mode Short Duration Power Limit (also known as Power Limit PL2) in Watts. The value may vary from 0 to Fused Value. If the value is 0, the fused value will be programmed. A value greater than fused TDP value will not be programmed |
| - Short Duration Turbo Mode   | Enabled<br>Disabled                    | Enable/Disable Short Duration Turbo Mode for processor   |
| - Energy Efficient Enable     | Enabled<br>Disabled                    | Enable/Disable Energy Efficient for processor  |
| Configure TDP Boot Mode       | Nominal<br>Down<br>Up<br>Disabled      | Configure TDP Mode (cTDP). Disabled option will skip all cTDP boot configurations  |

|                              |  |  |
|------------------------------|--|--|
| Lock TDP Settings            | <b>Disabled</b><br>Enabled               | Lock TDP in MSR_CONFIG_TDP_CONTROL                               |
| C-States                     | <b>Enabled</b><br>Disabled               | Enable processor idle power saving states                        |
| - Extend C-States            | <b>Enabled</b><br>Disabled               | Enable C-State transitions to occur in combination with P-States |
| - C3 State                   | <b>Enabled</b><br>Disabled               | Enable processor idle power saving C3 state                      |
| - C6 State                   | <b>Enabled</b><br>Disabled               | Enable processor idle power saving C6 state                      |
| - C6 Latency                 | <b>Short</b><br>Long                     | Configure Short/Long latency                                     |
| - C7 State                   | Disabled<br>C7<br><b>C7s</b>             | Enable processor idle power saving C7 state                      |
| - C7 Latency                 | <b>Short</b><br>Long                     | Configure Short/Long latency                                     |
| - C-State Auto Demotion      | Disabled<br>C1<br>C3<br><b>C1 and C3</b> | Configure C-State Auto Demotion                                  |
| - C-State Auto UnDemotion    | Disabled<br>C1<br>C3<br><b>C1 and C3</b> | Configure C-State Auto UnDemotion                                |
| - Package C-State Demotion   | <b>Disabled</b><br>Enabled               | Enable/Disable Package C-State Demotion                          |
| - Package C-State UnDemotion | <b>Disabled</b><br>Enabled               | Enable/Disable Package C-State UnDemotion                        |
| - C-State Pre-Wake           | <b>Enabled</b><br>Disabled               | Enable/Disable C-State Pre-Wake                                  |

## Miscellaneous

| Phoenix SecureCore Technology Setup                               |                    |
|---|--------------------|
| Advanced  |                    |
| Miscellaneous   | Item Specific Help |
| Miscellaneous Configuration                                       |                    |
| ▶ I2C Speed   |                    |
| ▶ Watchdog  |                    |
| ▶ Generic LPC Decode Ranges                                       |                    |
| S5 Eco  | [Disabled]         |
| Smart Battery Configuration                                       | [Disabled]         |
| Reset Button Behavior   | [Chipset Reset]    |
| Esc Exit → Select Menu Enter Select ▶ Sub-Menu F10 Save and Exits |                    |

| Feature                     | Options                                | Description   |
|-----------------------------|--|---|
| S5 Eco                      | Disabled<br>Enabled                    | Enable/Disable Kontron S5 Eco mode. Reduces supply current in Soft Off (S5) to less than 1mA. If enabled, power button is the only wake-up source in S5! See chapter S5 Eco for further details |
| Smart Battery Configuration | Disabled<br>Auto<br>Charger<br>Manager | Enable/Disable Smart Battery System Support (e.g. Kontron M.A.R.S.)   |
| Reset Button Behavior       | Chipset Reset<br>Power Cycle           | Select the system behavior on reset button event  |

## I2C Speed

| Phoenix SecureCore Technology Setup                                     |  |
|---|--|
| Advanced  |  |
| I2C Speed   | Item Specific Help   |
| I2C Bus Configuration<br>I2C Speed                    [200]             | Select I2C Bus Speed in kHz, min. 1kHz, max. 400kHz. For a default system 200kHz should be an appropriate value. |
| Esc Exit   ← Select Menu   Enter Select ► Sub-Menu   F10 Save and Exits |  |

| Feature   | Options | Description                                     |
|-----------|---------|---|
| I2C Speed | 200     | Select I2C Bus Speed in kHz from 1kHz to 400kHz |

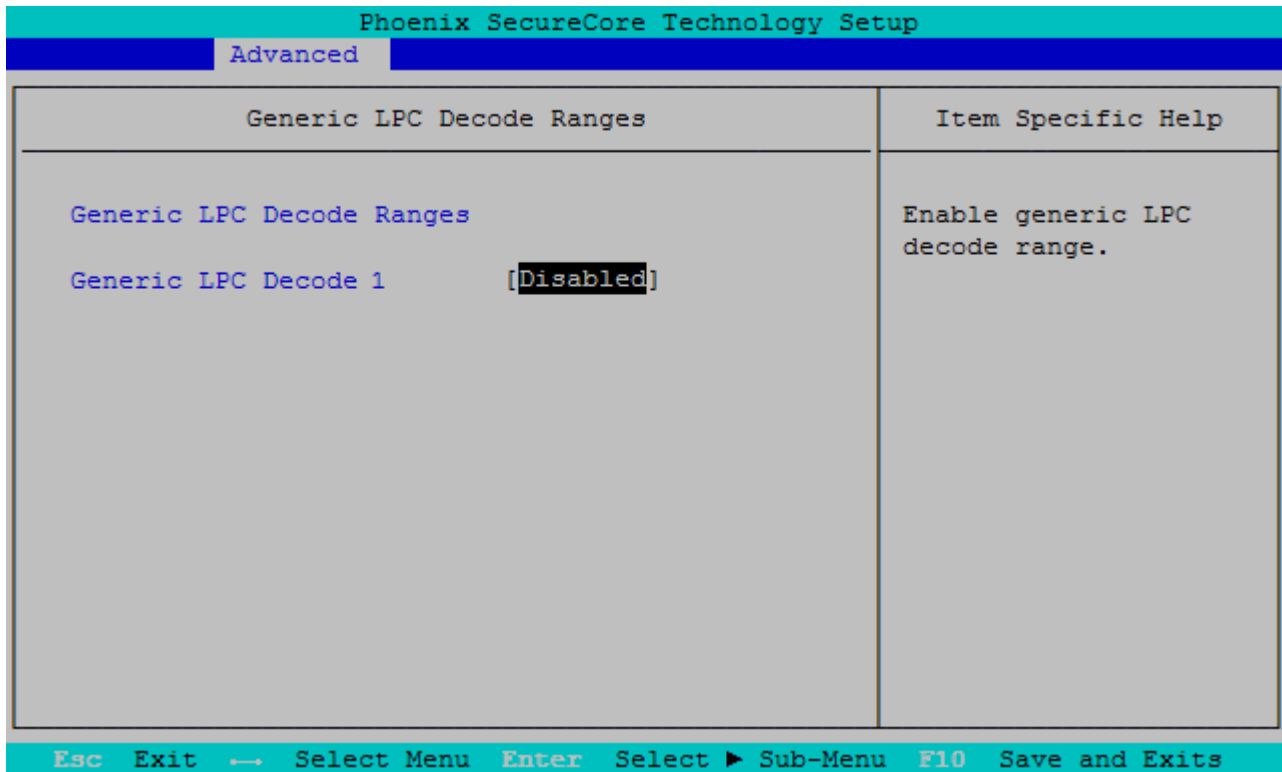
## Watchdog

| Phoenix SecureCore Technology Setup  |  |
|--|--|
| Advanced   |  |
| Watchdog   | Item Specific Help                                     |
| Watchdog Configuration.<br>Auto-reload [Disabled]<br>Global Lock [Disabled]<br><br>Stage 1 Mode [Disabled] | Enable automatic reload of watchdog timers on timeout. |
| Esc Exit ← Select Menu Enter Select ► Sub-Menu F10 Save and Exits  |  |

| Feature             | Options   | Description  |
|---------------------|---|--|
| Auto-reload         | Disabled<br>Enabled                                     | Enable automatic reload of watchdog timers on timeout  |
| Global Lock         | Disabled<br>Enabled                                     | If set to enabled, all Watchdog registers (except WD_KICK) become read only until the board is reset |
| Stage 1 Mode        | Disabled<br>Reset<br>NMI<br>SCI                         | Select Action for first Watchdog stage   |
| - Assert WDT Signal | Enabled<br>Disabled                                     | Enable/Disable assertion of WDT signal to baseboard on stage timeout                                 |
| - Stage 1 Timeout   | 1s<br>5s<br>10s<br><b>30s</b><br>1m<br>3m<br>10m<br>30m | Select Timeout value for first watchdog stage  |
| Stage 2 Mode        | Disabled<br>Reset<br>NMI<br>SCI                         | Select Action for first Watchdog stage   |
| - Assert WDT Signal | Disabled<br>Enabled                                     | Enable/Disable assertion of WDT signal to baseboard on stage timeout                                 |
| - Stage 2 Timeout   | 1s<br>5s<br>10s<br><b>30s</b><br>1m<br>3m<br>10m<br>30m | Select Timeout value for second watchdog stage   |



## Generic LPC Decode Ranges



| Feature              | Options             | Description   |
|----------------------|---------------------|---|
| Generic LPC Decode 1 | Disabled<br>Enabled | Enable generic LPC decode range   |
| - Base Address       | 0100h               | Base address of the generic decode range. Valid between 0100h - FFF0h. Must be 8-byte aligned |
| - Length             | 0008h               | Length of the generic decode range. Valid between 0800h - 0100h. Must be multiple of 8.       |
| Generic LPC Decode 2 | Disabled<br>Enabled | Enable generic LPC decode range   |
| - Base Address       | 0100h               | Base address of the generic decode range. Valid between 0100h - FFF0h. Must be 8-byte aligned |
| - Length             | 0008h               | Length of the generic decode range. Valid between 0800h - 0100h. Must be multiple of 8.       |
| Generic LPC Decode 3 | Disabled<br>Enabled | Enable generic LPC decode range   |
| - Base Address       | 0100h               | Base address of the generic decode range. Valid between 0100h - FFF0h. Must be 8-byte aligned |
| - Length             | 0008h               | Length of the generic decode range. Valid between 0800h - 0100h. Must be multiple of 8.       |

## H/W Monitor

Phoenix SecureCore Technology Setup

Advanced

| H/W Monitor NCT7802Y   | Item Specific Help |
|--|--------------------|
| <p>Temperature Measurement</p> <p><b>CPU Temperature</b> [ +69 C]</p> <p><b>PCH Temperature</b> [ +42 C]</p> <p><b>Module Temperature</b> [ +32 C]</p> <p>Fan Measurement</p> <p><b>CPU Fan</b> [ 1232 RPM]</p> <p>Fan Pulse [2]</p> <p>Fan Control [Auto]</p> <p>Fan Trip Point [45]</p> <p>Trip Point Speed [ 50]</p> <p>Reference Temperature [CPU Temperature]</p> <p><b>External Fan</b> [ 1274 RPM]</p> <p>Fan Pulse [2]</p> <p>Fan Control [Auto]</p> <p>Fan Trip Point [45]</p> <p>Trip Point Speed [ 50]</p> <p>Reference Temperature [CPU Temperature]</p> <p>Voltage Measurement</p> <p><b>Widerange Vcc</b> [ +12.03 V]</p> <p><b>5.0V Standby</b> [ +5.18 V]</p> <p><b>Batt volt at COMe pin</b> [ +3.05 V]</p> |                    |
| <p>Esc Exit ← Select Menu Enter Select ► Sub-Menu F10 Save and Exits</p>   |                    |


| Feature               | Value/Options   | Description  |
|-----------------------|---|--|
| CPU Temperature       | xx°C  | Shows the measured temperature of the CPU Diode with onboard HWM                           |
| PCH Temperature       | xx°C  | Shows the internal Platform Controller Hub temperature                                     |
| Module Temperature    | xx°C  | Shows the internal hardware-monitor temperature  |
| CPU FAN               | xxxx rpm  | Shows the fan speed of onboard FAN connector   |
| Fan Pulse             | 2   | Number of pulses the CPU fan produces during one revolution. Range 1-4                     |
| FAN Control           | Disabled<br>Manual<br><b>Auto</b>                               | Set fan control mode. 'Disable' will totally stop the fan                                  |
| Fan Trip Point        | 45  | Temperature where fan accelerates. Range 20 - 80°C   |
| Fan Speed             | 70  | Manual fan speed in %. Minimum value is 30 (in Manual mode only)                           |
| Trip Point Speed      | 50  | Fan speed at trip point in %. Minimum value is 30. Fan always runs at 100% at Tjmax - 10°C |
| Reference Temperature | <b>CPU Temperature</b><br>PCH Temperature<br>Module Temperature | Determines the temperature source which is used for automatic fan control                  |
| External FAN          | xxxx rpm  | Shows the fan speed of external COMe FAN   |
| Fan Pulse             | 2   | Select the number of pulses the external fan produces during one revolution. Range 1-4     |
| FAN Control           | Disabled<br>Manual<br><b>Auto</b>                               | Set fan control mode. 'Disable' will totally stop the fan                                  |
| Fan Trip Point        | 45  | Temperature where fan accelerates. Range 20 - 80°C   |
| Fan Speed             | 70  | Manual fan speed in %. Minimum value is 30 (in Manual mode only)                           |
| Trip Point Speed      | 50  | Fan speed at trip point in %. Minimum value is 30. Fan always runs at 100% at Tjmax - 10°C |

|                       |   |   |
|-----------------------|---|---|
| Reference Temperature | PCH Temperature<br>Module Temperature<br><b>CPU Temperature</b> | Determines the temperature source which is used for automatic fan control |
| Widerange Vcc         | x.xx V  | Shows the Module Main Input Voltage                                       |
| 5.0V Standby          | x.xx V  | Shows the 5V Standby Voltage input  |
| Batt volt at COMe pin | x.xx V  | Shows the RTC Battery Voltage input measured at COMe connector            |

## HDD Configuration

Phoenix SecureCore Technology Setup

Advanced

| HDD Configuration                           | Item Specific Help  |
|---|---|
| SATA Device [Enabled]                       |  |
| Interface Combination [AHCI]                |   |
| Aggressive Link Power [Enabled]             |   |
| SATA Speed [Gen. 2]                         |   |
| ▶ Software Feature Mask Configuration       |   |
| ComExpress SATA 0 Not Installed or the port |   |
| Port Enable [Enabled]                       |   |
| Hot Plug [Disabled]                         |   |
| SATA Device Type [Hard Disk Drive]          |   |
| ComExpress SATA 1 Not Installed or the port |   |
| Port Enable [Enabled]                       |   |
| Hot Plug [Disabled]                         |   |
| SATA Device Type [Hard Disk Drive]          |   |
| ComExpress SATA 2 Not Installed or the port |   |
| Port Enable [Enabled]                       |   |
| Hot Plug [Disabled]                         |   |
| SATA Device Type [Hard Disk Drive]          |   |
| ComExpress SATA 3 Not Installed or the port |   |
| Port Enable [Enabled]                       |   |
| Hot Plug [Disabled]                         |   |
| SATA Device Type [Hard Disk Drive]          |   |

Esc Exit → Select Menu Enter Select ▶ Sub-Menu F10 Save and Exits

| Feature               | Options                                     | Description   |
|-----------------------|---|---|
| SATA Device           | Enabled<br>Disabled                         | Enable/Disable SATA Device  |
| Interface Combination | IDE<br><b>AHCI</b><br>RAID                  | Select the SATA controllers operation mode                                  |
| Aggressive Link Power | Disabled<br><b>Enabled</b>                  | If enabled, turns on Aggressive Link Power Management on all HDD ports      |
| SATA Speed            | Gen1<br><b>Gen2</b><br>Gen3                 | Select the supported SATA speed mode  |
| Port Enable           | <b>Enabled</b><br>Disabled                  | Enable or Disable SATA Port   |
| Hot Plug              | <b>Disabled</b><br>Enabled                  | Designates this port as Hot Pluggable. Requires hardware support            |
| SATA Device Type      | <b>Hard Disk Drive</b><br>Solid State Drive | Identify the SATA port is connected to Solid State Drive or Hard Disk Drive |

## Software Feature Mask Configuration

| Phoenix SecureCore Technology Setup                               |  |
|---|--|
| Advanced  |  |
| HDD Configuration   | Item Specific Help   |
| HDD Unlock [Enabled]<br>LED Locate [Enabled]                      | If enabled, indicates that the HDD password unlock in the OS is enabled. |
| Esc Exit ← Select Menu Enter Select ► Sub-Menu F10 Save and Exits |  |

| Feature    | Options             | Description   |
|------------|---------------------|---|
| HDD Unlock | Enabled<br>Disabled | If enabled, indicates that the HDD password unlock in the OS is enabled                                       |
| LED Locate | Enabled<br>Disabled | If enabled, indicates that the LED/SGPIO hardware is attached and ping to locate feature is enabled on the OS |

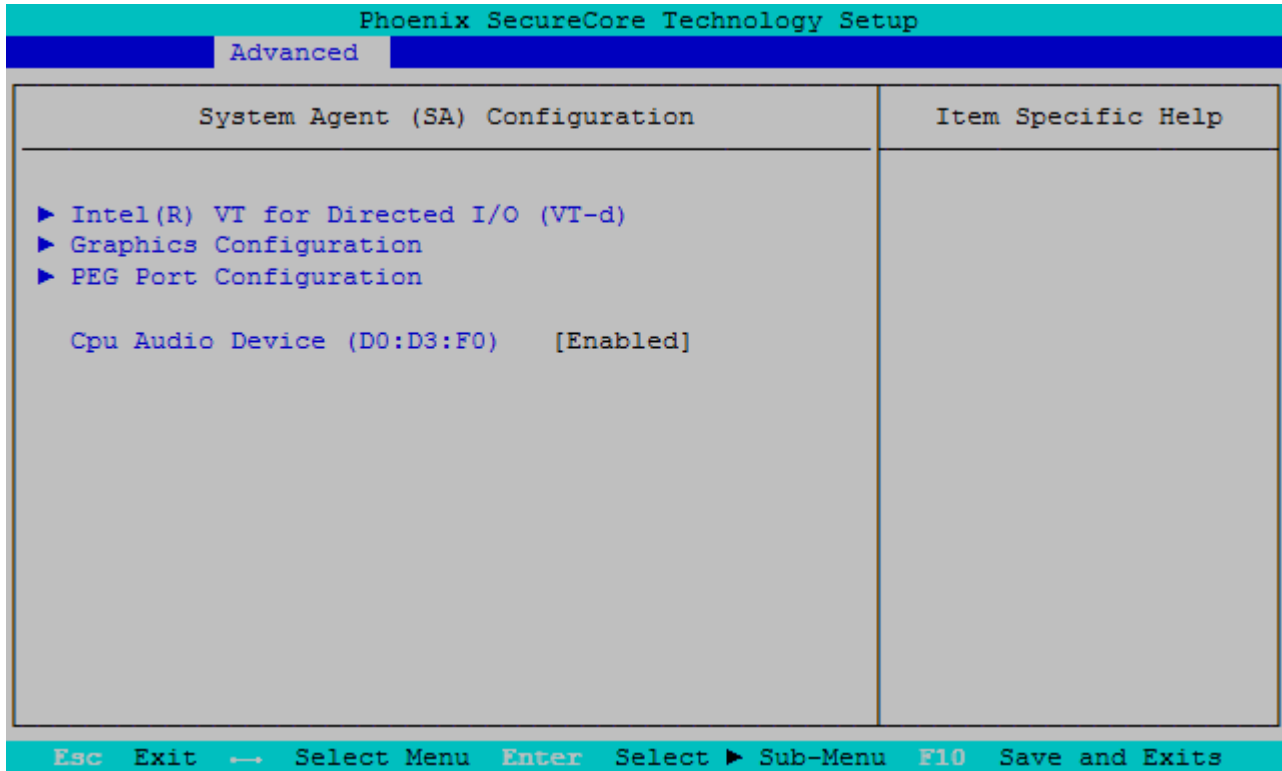
## Memory Configuration

| Phoenix SecureCore Technology Setup |                   |   |
|-------------------------------------|-------------------|---|
| Advanced                            |                   |   |
| Memory Configuration                |                   | Item Specific Help                          |
| Memory Frequency Limiter            | [Auto]            | Maximum Memory Frequency Selections in Mhz. |
| Max TOLUD                           | [Dynamic]         |   |
| NMode Support                       | [Auto]            |   |
| Channel A DIMM Control              | [Enabled]         |   |
| Channel B DIMM Control              | [Enabled]         |   |
| Memory Remap                        | [Enabled]         |   |
| MRC FastBoot                        | [Enabled]         |   |
| DIMM Profile                        | [Default profile] |   |

Esc Exit → Select Menu Enter Select ► Sub-Menu F10 Save and Exits

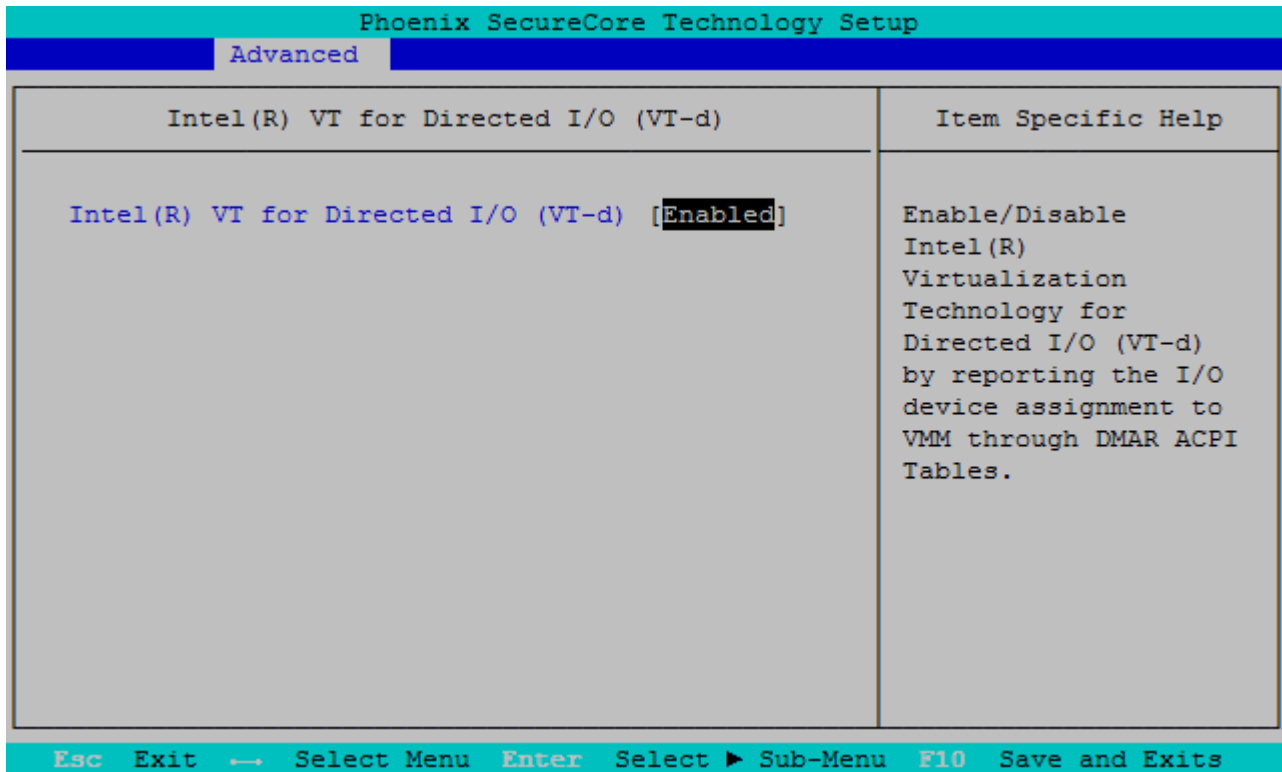
| Feature                  | Options   | Description   |
|--------------------------|---|---|
| Memory Frequency Limiter | <b>Auto</b><br>2067<br>1333<br>1600<br>1867<br>2133<br>2400<br>2667 | Select the memory frequency in MHz  |
| Max TOLUD                | <b>Dynamic</b><br>1 GB ... 3.25GB                                   | Maximum Value of TOLUD. Dynamic assignment would adjust TOLUD automatically based on largest MMIO length of installed graphic controller. Manual TOLUD setting from 1GB to 3.25GB in 0.25GB steps |
| NMode Support            | <b>Auto</b><br>1N Mode<br>2N Mode                                   | Select the memory supported Command Rate (N-Mode)   |
| Channel A DIMM Control   | <b>Enabled</b><br>Disabled  | Enables or disables DIMMs on channel A  |
| Channel B DIMM Control   | <b>Enabled</b><br>Disabled  | Enables or disables DIMMs on channel B  |
| Memory Remap             | <b>Enabled</b><br>Disabled  | Enable/Disable Memory Remap above 4GB   |
| MRC FastBoot             | <b>Enabled</b><br>Disabled  | Enable/Disable MRC FastBoot. Generally, this option only takes effect when doing cold boots/resets  |
| DIMM Profile             | <b>Default DIMM profile</b><br>XMP profile 1<br>XMP Profile 2       | Select Intel Extreme Memory Profile XMP if supported by DIMM SPD  |

## System Agent (SA) Configuration



| Feature                     | Options             | Description                     |
|-----------------------------|---------------------|---------------------------------|
| CPU Audio Device (D0:D3:F0) | Enabled<br>Disabled | Enable/Disable CPU Audio Device |

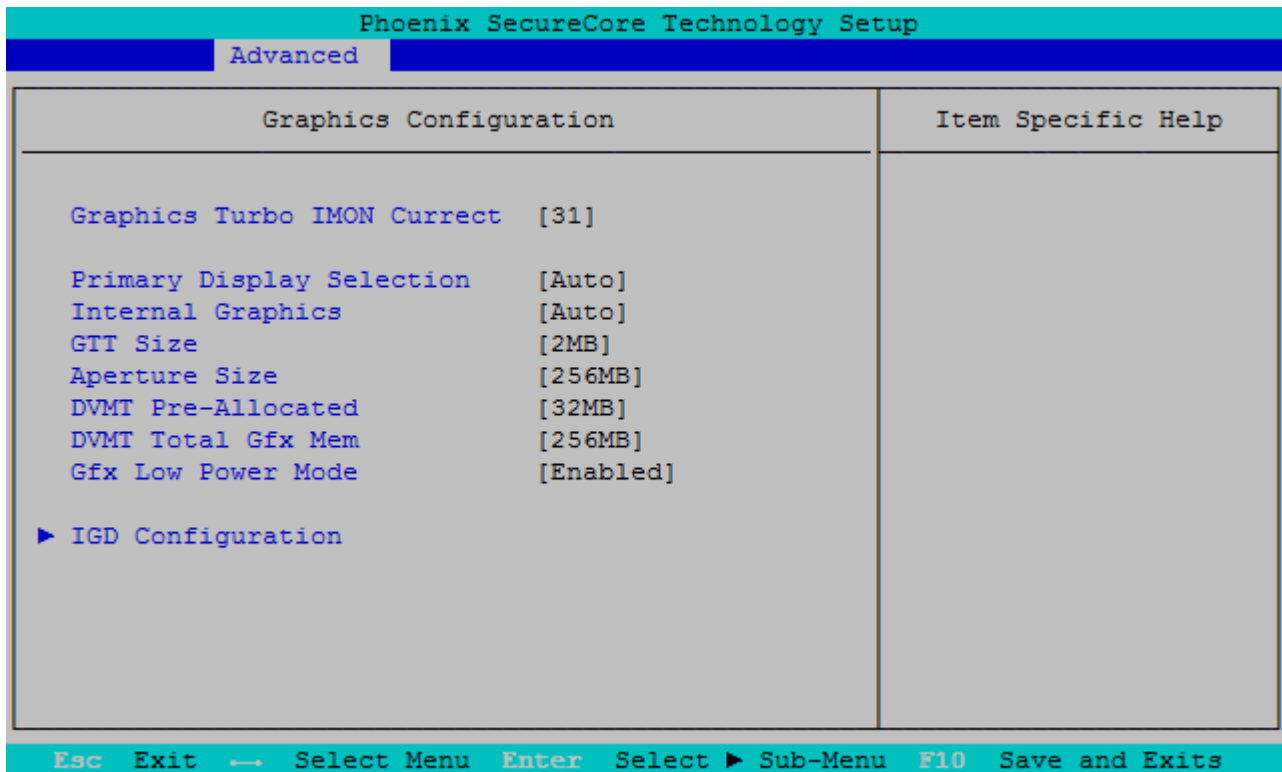
## Intel® VT for Directed I/O (VT-d)



| Feature                           | Options             | Description   |
|-----------------------------------|---------------------|---|
| Intel® VT for Directed I/O (VT-d) | Enabled<br>Disabled | Enable/Disable Intel Virtualization Technology for Directed I/O (VT-d) by reporting the I/O device assignment to VMM through DMAR ACPI Tables |



## Graphics Configuration



| Feature                     | Options                            | Description  |
|-----------------------------|------------------------------------|--|
| Graphics Turbo IMON Current | 31                                 | Graphics turbo IMON current value supported (14-31)  |
| Primary Display Selection   | IGD<br>PEG<br>PCI<br><b>Auto</b>   | Select the primary display device  |
| Internal Graphics           | Disabled<br>Enabled<br><b>Auto</b> | Enable/Disable the Internal Graphics Device. This has no effect if external graphics are present |
| GTT Size                    | 1MB<br><b>2MB</b>                  | Select the GTT Memory Size of IGD  |
| Aperture Size               | 128MB<br><b>256MB</b><br>512MB     | Select the Graphics Aperture Size  |
| DVMT Pre-Allocated          | <b>32MB</b><br>64MB<br>128MB       | Select Pre-Allocated Graphics Memory size used by the Internal Graphics device                   |
| DVMT Total Gfx Mem          | 128MB<br><b>256MB</b><br>Max       | Select the maximum DVMT5.0 Graphics Memory Size  |
| GFX Low Power Mode          | <b>Enabled</b><br>Disabled         | Enable/Disable Gfx Low Power Mode  |

## IGD Configuration

| Phoenix SecureCore Technology Setup |                    |                    |
|-------------------------------------|--------------------|--------------------|
| Advanced                            |                    |                    |
| IGD Configuration                   |                    | Item Specific Help |
| IGD - Boot Type                     | [Auto]             |                    |
| Backlight Control                   | [I2C]              |                    |
| Backlight Value                     | [128]              |                    |
| eDP Panel Type                      | [LVDS]             |                    |
| LVDS Clock Center Spreading         | [No Spreading]     |                    |
| EFP1 Type                           | [DP with HDMI/DVI] |                    |
| EFP2 Type                           | [DP with HDMI/DVI] |                    |
| EFP3 Type                           | [DP with HDMI/DVI] |                    |
| Mode Persistence                    | [Disabled]         |                    |

Esc Exit ← Select Menu Enter Select ► Sub-Menu F10 Save and Exits

| Feature                     | Options   | Description   |
|-----------------------------|---|---|
| IGD - Boot Type             | <b>Auto</b><br>CRT<br>EFP<br>LFP<br>EFP3<br>EFP2  | Select the Integrated Graphics Video Device which will be activated during POST           |
| IGD - Secondary Boot Type   | <b>Disabled</b><br>CRT<br>EFP<br>LFP<br>EFP3<br>EFP2  | Select the second Video Device which will be activated during POST                        |
| LFP Type                    | <b>AUTO</b><br>VGA 640×480 1×18<br>WVGA 800×480 1×18<br>SVGA 800×600 1×18<br>XGA 1024×768 1×18<br>XGA 1024×768 1×24<br>WXGA 1280×768 1×24<br>WXGA 1280×800 1×18<br>WXGA 1366×768 1×24<br>WXGA+ 1440×900 2×18<br>WXGA+ 1440×900 2×24<br>SXGA 1280×1024 2×18<br>SXGA 1280×1024 2×24<br>WSXGA+ 1680×1050 2×18<br>WSXGA+ 1680×1050 2×24<br>UXGA 1600×1200 2×18<br>UXGA 1600×1200 2×24<br>WUXGA 1920×1200 2×18<br>WUXGA 1920×1200 2×24<br>Custom | Select LFP used by Internal Graphics Device by selecting the appropriate panel setup item |
| Backlight Control           | None/External<br>PWM<br>PWM Inverted<br><b>I2C</b>  | Backlight Control Setting   |
| Backlight Value             | <b>128</b>  | Set LCD backlight brightness (0-255)  |
| eDP Panel Type              | <b>LVDS</b><br>eDP  | Select Panel Type connected to eDP Port (eDP only available with customized hardware)     |
| LVDS Clock Center Spreading | <b>No Spreading</b><br>0.5%<br>1.0%<br>1.5%<br>2.0%<br>2.5%   | Select LVDS clock frequency center spreading depth  |
| EFP1 Type                   | DisplayPort Only  | Integrated HDMI/DisplayPort Configuration with  |

|                        |  |                                   |
|------------------------|--|-----------------------------------|
| EFP2 Type<br>EFP3 Type | <b>DP with HDMI/DVI</b><br>DP with DVI<br>HDMI/DVI | External Connectors               |
| Mode Persistence       | <b>Disabled</b><br>Enabled                         | Enables/Disables Mode Persistence |

## PEG Port Configuration

**Phoenix SecureCore Technology Setup**

**Advanced**

| PEG Port Configuration                        | Item Specific Help |
|---|--------------------|
| PEG Configuration [1x16]                      | ▲<br>↓             |
| PEG0 - Gen X [Auto]                           |                    |
| Always Enable PEG [Disabled]                  |                    |
| PEG ASPM [Auto]                               |                    |
| Program PCIe ASPM later than OpROM [Disabled] |                    |
| De-emphasis Control [-3.5 dB]                 |                    |
| Swing Control [Full]                          |                    |
| PEG Sample Calibrate [Auto]                   |                    |
| Gen3 Equalization [Enabled]                   |                    |
| PEG Gen3 Equalization Phase2 [Disabled]       |                    |
| Gen3 Root Port Preset [ 8]                    |                    |
| Gen3 Endpoint Preset [ 7]                     |                    |
| Gen3 Endpoint Hint [ 2]                       |                    |
| Gen3 Eq Preset Search [Enabled]               |                    |
| Always re-search Gen3 Eq Preset [Disabled]    |                    |
| Allow PREST# GPIO Usage [Disabled]            |                    |
| Preset Search Dwell Time [ 1000]              |                    |
| Timing Start Margin [ 15]                     |                    |
| Voltage Start Margin [ 20]                    |                    |
| Error Target [ 1]                             |                    |
| PEG RxCEM Loopback Mode [Disabled]            |                    |
| PEG Gen3 RxCTLE Control [ 8]                  |                    |

**Esc Exit ← Select Menu Enter Select ▶ Sub-Menu F10 Save and Exits**

| Feature                            | Options                                     | Description  |
|------------------------------------|---|--|
| PEG Configuration                  | 1x16<br>2x8<br>1x8 + 1x4                    | Set PEG Configuration to 1x16, 2x8 or 1x8 + 2x4  |
| PEG0 - Gen X                       | Auto<br>Gen1<br>Gen2<br>Gen3                | Configure PEG0 B0:D1:F0 Speed  |
| Always Enable PEG                  | Disabled<br>Enabled                         | Enabled: PEG is always on. Disabled: PEG is only enabled with connected PCIe device        |
| PEG ASPM                           | Disabled<br>LOs<br>L1<br>LOs and L1<br>Auto | Control ASPM support for the PEG Device  |
| Program PCIe ASPM later than OpROM | Disabled<br>Enabled                         | Select whether the PCIe ASPM will be programmed before (disabled) or after (enabled) OpROM |
| De-emphasis Control                | -6 dB<br>-3.5 dB                            | Configure the De-emphasis control on PEG   |
| Swing Control                      | Reduced<br>Half<br>Full                     | Perform PEG Swing Control  |
| PEG Sample Calibrate               | Disabled<br>Enabled<br>Auto                 | Enable/Disable PEG Sample Calibrate  |
| Gen3 Equalization                  | Disabled<br>Enabled                         | Perform PEG Gen3 Equalization steps  |
| PEG Gen3 Equalization Phase2       | Disabled<br>Enabled                         | Enable/Disable PEG Gen3 Equalization Phase2  |
| Gen3 Root Port Preset              | 8   | Root port preset value for Gen3 Equalization   |
| Gen3 Endpoint Preset               | 7   | Endpoint preset value for Gen3 Equalization  |

|                                 |                            |   |
|---------------------------------|----------------------------|---|
| Gen3 Endpoint Hint              | <b>2</b>                   | Endpoint Hint value for Gen3 Equalization   |
| Gen3 Eq Preset Search           | Disabled<br><b>Enabled</b> | Perform PEG Gen3 SW Preset Search algorithm   |
| Always re-search Gen3 Eq Preset | <b>Disabled</b><br>Enabled | Always re-search PEG Gen3 Preset, even it has been done once                        |
| Allow PREST# GPIO Usage         | <b>Disabled</b><br>Enabled | Enable/Disable GPIO-based resets to PEG endpoint(S) during margin search, if needed |
| Preset Search Dwell Time        | <b>1000</b>                | PEG Gen3 Preset Search dwell time in (ms)   |
| Timing Start Margin             | <b>15</b>                  | The starting value (4 ... 255) for the backward margin search                       |
| Voltage Start Margin            | <b>20</b>                  | The starting value (4 ... 255) for the backward margin search                       |
| Error Target                    | <b>1</b>                   | The margin search errortarget value (1 ... 65535)                                   |
| PEG RxCEM Loopback Mode         | <b>Disabled</b><br>Enabled | Enable/Disable PEG RxCEM Loopback Mode  |
| PEG Gen3 RxCTLE Control         | <b>8</b>                   | PEG Gen3 RxCTLE setting for Bundle0 (Lane0, Lane1)                                  |

## South Bridge Configuration

| Phoenix SecureCore Technology Setup   |                    |
|---|--------------------|
| Advanced  |                    |
| South Bridge Configuration  | Item Specific Help |
| SMBUS Device [Enabled]<br>State After G3 [State S0]<br>▶ SB PCI Express Config<br>▶ SB USB Config<br>▶ SB Azalia Config |                    |
| Esc Exit ← Select Menu Enter Select ▶ Sub-Menu F10 Save and Exits   |                    |

| Feature        | Options                                   | Description  |
|----------------|---|--|
| SMBUS Device   | Disabled<br><b>Enabled</b>                | Enable/Disable SMBUS Device  |
| State After G3 | State S5<br><b>State S0</b><br>Last State | Specify what state to switch to when power is re-applied after a power failure (G3 state). S5 = Stay Off, S0 = switch on |

## SB PCI Express Config

Phoenix SecureCore Technology Setup

Advanced

| SB PCI Express Config   | Item Specific Help |
|---|--------------------|
| PCI Express Root Port Clock Gating [Enabled]<br>DMI Link ASPM Control [LOS]<br>DMI Link Extended Synch Control [Disabled]<br><b>PCI Express port assigned to LAN 8</b><br><br>▶ PCI Express Port 1 Config<br>▶ PCI Express Port 2 Config<br>▶ PCI Express Port 3 Config<br>▶ PCI Express Port 4 Config<br>▶ PCI Express Port 5 Config<br>▶ PCI Express Port 6 Config<br>▶ PCI Express Port 7 Config<br><br>PCI ExpressCard 0 [Disabled]<br>PCI ExpressCard 1 [Disabled] |                    |

Esc Exit ← Select Menu Enter Select ▶ Sub-Menu F10 Save and Exits

| Feature                                | Options   | Description  |
|--|---|--|
| PCIe Root Port Clock Gating            | Disabled<br><b>Enabled</b>  | Enable or Disable PCI Express Clock Gating for each root port                      |
| DMI Link ASPM Control                  | Disabled<br><b>Enabled</b>  | Controls Active State Power Management on both NB side and SB side of the DMI Link |
| DMI Link Ext Synch                     | <b>Disabled</b><br>Enabled  | Controls Extended Synch on SB side of the DMI Link                                 |
| PCIe-USB Glitch W/A                    | Disabled<br><b>Enabled</b>  | PCIe-USB Glitch W/A for bad USB device(s) connected behind PCIe/PEG Port           |
| PCI ExpressCard 0<br>PCI ExpressCard 1 | Port 0<br>Port 1<br>Port 2<br>Port 3<br>Port 4<br>Port 5<br>Port 6<br>Port 7<br><b>Disabled</b> | Controls PCIe Port for ExpressCard support   |



## PCI Express Root Port 0/1/2/3/4/5/6

| Phoenix SecureCore Technology Setup |               |                                    |
|-------------------------------------|---------------|------------------------------------|
| Advanced                            |               |                                    |
| PCI Express Root Port 1             |               | Item Specific Help                 |
| PCI Express Root Port 1             | [Enabled]     | Control the PCI Express Root Port. |
| PCIe Speed                          | [Auto]        |                                    |
| ASPM                                | [Auto]        |                                    |
| L1 Substates                        | [L1.1 & L1.2] |                                    |
| HOT PLUG                            | [Disabled]    |                                    |
| URR                                 | [Disabled]    |                                    |
| FER                                 | [Disabled]    |                                    |
| NFER                                | [Disabled]    |                                    |
| CER                                 | [Disabled]    |                                    |
| SEFE                                | [Disabled]    |                                    |
| SENF                                | [Disabled]    |                                    |
| SECE                                | [Disabled]    |                                    |
| PME Interrupt                       | [Disabled]    |                                    |
| PME SCI                             | [Enabled]     |                                    |

Esc Exit ← Select Menu Enter Select ► Sub-Menu F10 Save and Exits

| Feature                 | Options  | Description   |
|-------------------------|--|---|
| PCI Express Root Port # | Disabled<br><b>Enabled</b>                         | Control the PCI Express Root Port                   |
| PCIe Speed              | <b>Auto</b><br>Gen1<br>Gen2                        | Select PCIe Speed to Gen1 or Gen2                   |
| ASPM                    | Disabled<br>LOs<br>L1<br>LOs and L1<br><b>Auto</b> | Control PCIe Active State Power Management settings |
| L1 Substates            | Disabled<br>L1.1<br>L1.2<br>L1.1 & L1.2            | PCI Express L1 Substates setting                    |
| HOT PLUG                | <b>Disabled</b><br>Enabled                         | PCI Express Hot Plug Enabled/Disabled               |
| URR                     | <b>Disabled</b><br>Enabled                         | PCI Express Unsupported Request Reporting           |
| FER                     | <b>Disabled</b><br>Enabled                         | PCI Express Device Fatal Error Reporting            |
| NFER                    | <b>Disabled</b><br>Enabled                         | PCI Express Device Non-Fatal Error Reporting        |
| CER                     | <b>Disabled</b><br>Enabled                         | PCI Express Device Correctable Error Reporting      |
| SEFE                    | <b>Disabled</b><br>Enabled                         | PCI Express System Error on Fatal Error             |
| SENF                    | <b>Disabled</b><br>Enabled                         | PCI Express System Error on Non-Fatal Error         |
| SECE                    | <b>Disabled</b><br>Enabled                         | PCI Express System Error on Correctable Error       |
| PME Interrupt           | <b>Disabled</b><br>Enabled                         | Root PCI Express PME Interrupt                      |
| PME SCI                 | Disabled<br><b>Enabled</b>                         | PCI Express PME SCI                                 |

## SB USB Config

| Phoenix SecureCore Technology Setup |              |   |
|-------------------------------------|--------------|---|
| Advanced                            |              |   |
| SB USB Configuration                |              | Item Specific Help  |
| USB Precondition                    | [Enabled]    | Precondition work on USB host controller and root ports for faster enumeration. |
| xHCI Mode                           | [Smart Auto] |   |
| Trunk Clock Gating (BTCG)           | [Enabled]    |   |
| EHCI1                               | [Enabled]    |   |
| EHCI2                               | [Enabled]    |   |
| USB Per-Port Disable Control        | [Disabled]   |   |

Esc Exit ← Select Menu Enter Select ► Sub-Menu F10 Save and Exits

| Feature  | Options  | Description  |
|--|--|--|
| USB Precondition   | Disabled<br><b>Enabled</b>                       | Precondition work on USB host controller and root ports for faster enumeration |
| xHCI Mode  | Disabled<br>Enabled<br>Auto<br><b>Smart Auto</b> | Mode of operation of xHCI controller   |
| Trunk Clock Gating (BTCG)  | Disabled<br><b>Enabled</b>                       | Enable/Disable BTCG  |
| EHCI1  | Disabled<br><b>Enabled</b>                       | Control the USB EHCI (USB2.0) functions for COMe Ports #0-3                    |
| EHCI2  | Disabled<br><b>Enabled</b>                       | Control the USB EHCI (USB2.0) functions for COMe Ports #4-7                    |
| USB Per-Port Disable Control   | <b>Disabled</b><br>Enabled                       | Controls each of the USB ports (0 ~ 13)  |
| - USB Port #0 Enable/Disable<br>- USB Port #1 Enable/Disable<br>- USB Port #2 Enable/Disable<br>- USB Port #3 Enable/Disable<br>- USB Port #4 Enable/Disable<br>- USB Port #5 Enable/Disable<br>- USB Port #6 Enable/Disable<br>- USB Port #7 Enable/Disable | Disabled<br><b>Enabled</b>                       | Enable/Disable USB port  |

## SB Azalia Config

| Phoenix SecureCore Technology Setup                               |   |
|---|---|
| Advanced  |   |
| SB Azalia Configuration   | Item Specific Help                      |
| Azalia [Auto]   | Control Detection of the Azalia device. |
| Esc Exit ← Select Menu Enter Select ► Sub-Menu F10 Save and Exits |   |

| Feature | Options             | Description                                     |
|---------|---------------------|---|
| Azalia  | Disabled<br>Enabled | Control Detection of the Azalia HD Audio Device |

## Network Configuration

| Phoenix SecureCore Technology Setup                               |                    |                                  |
|---|--------------------|----------------------------------|
| Advanced  |                    |                                  |
| Network Configuration   | Item Specific Help |                                  |
| PCH Internal LAN  | [Enabled]          | Enable/Disable PCH Internal LAN. |
| LAN OPROM Selection   | [Onboard only]     |                                  |
| Wake on PCH LAN   | [Enabled]          |                                  |
| ASF Support   | [Enabled]          |                                  |
| Esc Exit ← Select Menu Enter Select ► Sub-Menu F10 Save and Exits |                    |                                  |

| Feature             | Options   | Description   |
|---------------------|---|---|
| PCH Internal LAN    | Disabled<br><b>Enabled</b>                            | Enable/Disable PCH internal LAN                                       |
| LAN OPROM Selection | Disabled<br><b>Onboard only</b><br>Addon only<br>Both | This is used to select LAN OPROM for quick boot minimal configuration |
| Wake on PCH LAN     | Disabled<br><b>Enabled</b>                            | Enable PCH internal Wake on LAN capability                            |
| ASF Support         | Disabled<br><b>Enabled</b>                            | Enable/Disable Alert Specifications Format                            |

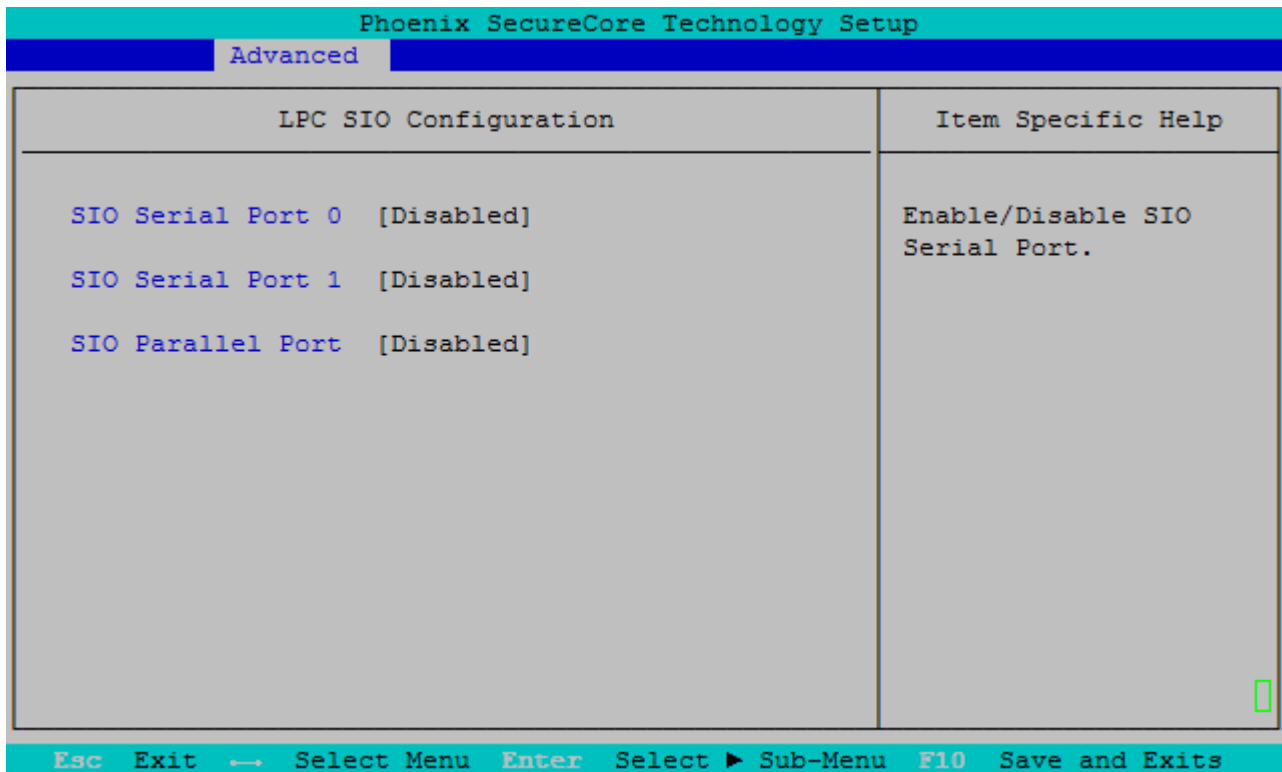
## CPLD Configuration

| Phoenix SecureCore Technology Setup                      |                             |
|--|-----------------------------|
| Advanced   |                             |
| Onboard UART configuration                               | Item Specific Help          |
| Serial Port 0 [Enabled]<br>Base Address [3F8]<br>IRQ [4] | Enable/Disable Serial Port. |
| Serial Port 1 [Enabled]<br>Base Address [2F8]<br>IRQ [3] |                             |

Esc Exit → Select Menu Enter Select ► Sub-Menu F10 Save and Exits

| Feature       | Options                            | Description                           |
|---------------|------------------------------------|---------------------------------------|
| Serial Port 0 | Disabled<br><b>Enabled</b>         | Enable or Disable Serial Port (COM) 0 |
| Base Address  | <b>3F8</b><br>2F8<br>3E8<br>2E8    | Configure Serial Port Base Address    |
| IRQ           | 3<br><b>4</b><br>5<br>6<br>7<br>12 | Configure Serial Port IRQ             |
| Serial Port 1 | Disabled<br><b>Enabled</b>         | Enable or Disable Serial Port (COM) 1 |
| Base Address  | 3F8<br><b>2F8</b><br>3E8<br>2E8    | Configure Serial Port Base Address    |
| IRQ           | <b>3</b><br>4<br>5<br>6<br>7<br>12 | Configure Serial Port IRQ             |
| GPIO IRQ      | <b>Disabled</b><br>14<br>15        | Configure IRQ for GPIO pins           |
| I2C IRQ       | <b>Disabled</b><br>14<br>15        | Configure IRQ for I2C controller      |

## LPC SIO Configuration



This setup option is only available with LPC SuperI/O Nuvoton 83627 present on the carrier board. By default the COMe-bHL6 supports the legacy interfaces of a 5V 83627HF(J) or 3.3V 83627DHG-P on external LPC. The SIO hardware monitor is not supported in setup.

|                   |  |                                      |
|-------------------|--|--------------------------------------|
| Serial Port 0     | <b>Disabled</b><br>Enabled   | Enable or Disable SIO Serial Port    |
| - Base Address    | 3F8<br>2F8<br><b>3E8</b><br>2E8  | Configure Serial Port Base Address   |
| - IRQ             | 3<br>4<br>5<br><b>6</b><br>7<br>12                                     | Configure Serial Port IRQ            |
| Serial Port 1     | <b>Disabled</b><br>Enabled   | Enable or Disable SIO Serial Port    |
| - Base Address    | 3F8<br>2F8<br>3E8<br><b>2E8</b>  | Configure Serial Port Base Address   |
| - IRQ             | 3<br>4<br>5<br>6<br><b>7</b><br>12                                     | Configure Serial Port IRQ            |
| SIO Parallel Port | <b>Disabled</b><br>Enabled   | Enable or Disable SIO Parallel Port  |
| - Device Mode     | <b>Standard Parallel Port</b><br>EPP<br>ECP & EPP 1.9<br>ECP & EPP 1.7 | Configure Parallel Port Mode         |
| - Base Address    | <b>378</b><br>278<br>3BC   | Configure Parallel Port Base Address |

## AMT Configuration (vPRO Version only)

| Phoenix SecureCore Technology Setup |                    |
|-------------------------------------|--------------------|
| Advanced                            |                    |
| AMT Configuration                   | Item Specific Help |
| Intel(R) AMT                        | [Enabled]          |
| AMT Wait Timer                      | [ 1 ]              |
| Activate Remote Assistance Process  | [Disabled]         |
| PET Progress                        | [Enabled]          |
| CIRA Trigger                        | [Enabled]          |
| AMT CIRA Timeout                    | [ 0 ]              |
| Watchdog                            | [Disabled]         |
| SOL Terminal Type                   | [VT100]            |
| Enable Redirection                  | [Enabled]          |
| Enable unsigned images on IDER boot | [Enabled]          |
| Enter Intel(R) MEBx Setup           | [Disabled]         |
| Un-Configure ME                     | [Disabled]         |
| Hide Un-Configure ME Confirmation   | [Disabled]         |
| MEBx Debug Message output           | [Disabled]         |
| USB Provision                       | [Enabled]          |
| ▶ MEBx Resolution Setting           |                    |

Esc Exit → Select Menu Enter Select ▶ Sub-Menu F10 Save and Exits

| Feature                             | Options                                | Description  |
|-------------------------------------|--|--|
| Intel® AMT                          | Disabled<br><b>Enabled</b>             | Enable/Disable Intel® Active Management Technology BIOS Extension. Note: iAMT H/W is always enabled. This option just controls the BIOS extension execution. |
| AMT Wait Timer                      | <b>1</b>                               | Set timer to wait before sending ASF_GET_BOOT_OPTIONS  |
| Active Remote Assistance Process    | <b>Disabled</b><br>Enabled             | Trigger CIRA boot  |
| PET Progress                        | Disabled<br><b>Enabled</b>             | Users can Enable/Disable PET Events progress to receive PET events or not  |
| CIRA Trigger                        | Disabled<br><b>Enabled</b>             | Enable/Disable Trigger for Remote Assistance Process using HotKey  |
| AMT CIRA Timeout                    | <b>0</b>                               | OEM defined timeout for the MPS connection to establish  |
| Watchdog                            | <b>Disabled</b><br>Enabled             | Enable/Disable Watchdog Timer  |
| - OS Timer                          | <b>1</b>                               | Set OS Watchdog timer  |
| - BIOS Timer                        | <b>1</b>                               | Set BIOS Watchdog timer  |
| SOL Terminal Type                   | ANSI<br><b>VT100</b><br>VT100+<br>UTF8 | Set Terminal Type for Serial Over LAN Sessions   |
| Enable Redirection                  | Disabled<br><b>Enabled</b>             | Enable/Disable Redirection   |
| Enable unsigned images on IDER boot | Disabled<br><b>Enabled</b>             | Enable the BIOS to boot from an unsigned image even when secure boot is enabled  |
| Enter Intel® MEBx Setup             | <b>Disabled</b><br>Enabled             | Enter Intel® MEBx Setup on the next boot   |
| Un-Configure ME                     | <b>Disabled</b><br>Enabled             | Un-Configure ME without a password   |
| Hide Un-Configure ME Confirmation   | <b>Disabled</b><br>Enabled             | Hide Un-Configure ME without password Confirmation Prompt  |
| MEBx Debug Message output           | <b>Disabled</b><br>Enabled             | Enable/Disable MEBx debug message output   |
| USB Provision                       | Disabled<br><b>Enabled</b>             | Enable/Disable USB Provision function  |

## MEBx Resolution Setting (vPRO Version only)

| Phoenix SecureCore Technology Setup  |   |
|--|---|
| Advanced   |   |
| MEBx Resolution Setting  | Item Specific Help  |
| Non-UI Text Mode resolution [Auto]<br>UI Text Mode resolution [Auto]<br>Graphic Mode Resolution [Auto] | Text Mode resolution used by MEBx for messages outside MEBx User Interface. |
| Esc Exit ← Select Menu Enter Select ► Sub-Menu F10 Save and Exits                                      |   |

| Feature                     | Options                                       | Description  |
|-----------------------------|---|--|
| Non-UI Text Mode resolution | <b>Auto</b><br>80×25<br>100×31                | Text Mode resolution used by MEBx for messages outside MEBx User Interface |
| UI Text Mode resolution     | <b>Auto</b><br>80×25<br>100×31                | Text Mode resolution used by MEBx to display the User Interface forms      |
| Graphic Mode resolution     | <b>Auto</b><br>640×480<br>800×600<br>1024×768 | Graphic Mode resolution used by MEBx to display boxes like consent sprite  |



## ME Configuration (default)

| Phoenix SecureCore Technology Setup                               |   |
|---|---|
| Advanced  |   |
| ME Configuration  | Item Specific Help                                      |
| ME FW Version 9.0.10.1372   | Configure Management<br>Engine Technology<br>Parameters |
| ME Firmware Intel(R)ME 1.5MB firmware                             |   |
| Esc Exit ← Select Menu Enter Select ► Sub-Menu F10 Save and Exits |   |

## ME Configuration (vPRO Version only)

| Phoenix SecureCore Technology Setup |                         |  |
|-------------------------------------|-------------------------|--|
| Advanced                            |                         |  |
| ME Configuration                    |                         | Item Specific Help                     |
| ME FW Version                       | 9.0.10.1372             | Enable/Disable ME Debug Event Service. |
| ME Firmware                         | Intel(R)ME SMB firmware |  |
| <b>Intel(R) ME</b>                  | <b>[Enabled]</b>        |  |
| ME Debug Event Service              | [Disabled]              |  |
| MDES for BIOS                       | [Disabled]              |  |
| ME IFR Feature                      | [Enabled]               |  |

Esc Exit → Select Menu Enter Select ► Sub-Menu F10 Save and Exits

| Feature                | Options             | Description   |
|------------------------|---------------------|---|
| ME Debug Event Service | Disabled<br>Enabled | Enable or Disable ME Debug Event Service                  |
| MDES for BIOS          | Disabled<br>Enabled | Enable or Disable ME Debug Event Service for BIOS events  |
| ME IFR Feature         | Disabled<br>Enabled | Enable or Disable Intel® ME Independent Firmware Recovery |

## Thermal Configuration

| Phoenix SecureCore Technology Setup  |                                    |
|--|------------------------------------|
| Advanced   |                                    |
| Thermal Configuration  | Item Specific Help                 |
| <ul style="list-style-type: none"><li>▶ CPU Thermal Configuration</li><li>▶ Platform Thermal Configuration</li></ul> | CPU Thermal Configuration Submenu. |

Esc Exit ← Select Menu Enter Select ▶ Sub-Menu F10 Save and Exits

## CPU Thermal Configuration

| Phoenix SecureCore Technology Setup |            |   |
|-------------------------------------|------------|---|
| Advanced                            |            |   |
| CPU Thermal Configuration           |            | Item Specific Help  |
| Thermal Monitor                     | [Enabled]  | Enable processor Thermal Monitor thermal control. Requires GV3. |
| Bi-directional PROCHOT#             | [Enabled]  |   |
| PROCHOT# OUT                        | [Disabled] |   |
| PROCHOT Response                    | [Disabled] |   |
| DTS                                 | [Enabled]  |   |

Esc Exit ← Select Menu Enter Select ► Sub-Menu F10 Save and Exits

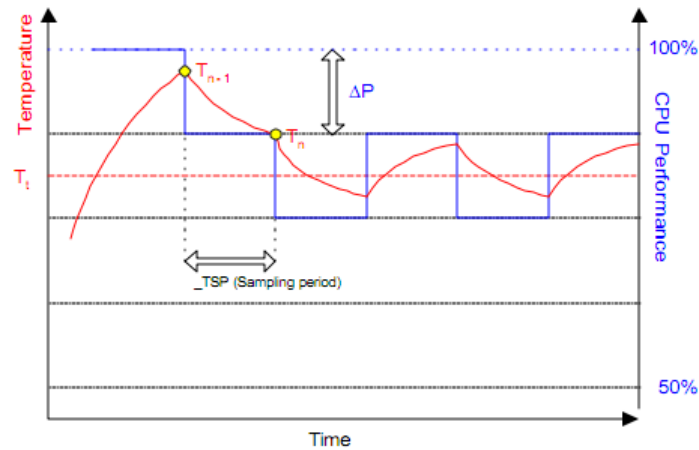
| Feature                 | Options                    | Description   |
|-------------------------|----------------------------|---|
| Thermal Monitor         | Disabled<br><b>Enabled</b> | Enable processor Thermal Monitor thermal control. Requires GV3  |
| Bi-directional PROCHOT# | Disabled<br><b>Enabled</b> | When a processor thermal sensor trips (either core), the PROCHOT# is driven. If bi-direction is enabled, external agents can drive PROCHOT# to throttle the processor |
| PROCHOT# OUT            | <b>Disabled</b><br>Enabled | If Bi-directional PROCHOT# is enabled, PROCHOT# OUT can be disabled selectively   |
| PROCHOT# Response       | <b>Disabled</b><br>Enabled | Enable/Disable PROCHOT Response   |
| DTS                     | Disabled<br><b>Enabled</b> | Enable CPU Digital Thermal Sensor function. DTS has to be enabled for ACPI Critical Shutdown and Passive Cooling  |

## Platform Thermal Configuration

| Phoenix SecureCore Technology Setup  |  |
|--|--|
| Advanced   |  |
| Platform Thermal Configuration   | Item Specific Help   |
| Critical Trip Point [POR]<br>Passive Trip Point [90 C]<br>Passive TC1 Value [ 1]<br>Passive TC2 Value [ 5]<br>Passive TSP Value [10] | This value controls the temperature of the ACPI critical Trip Point - the point where the OS shuts the system off. NOTE: 100C is the Plan of Record (POR) for all Intel mobile processors. |
| Esc Exit ← Select Menu Enter Select ► Sub-Menu F10 Save and Exits  |  |

| Feature             | Options                            | Description  |
|---------------------|------------------------------------|--|
| Critical Trip Point | <b>POR</b><br>15°C ... 95°C        | This value controls the temperature of the ACPI Critical Trip Point - the point where the OS shuts the system off. Note: 100°C is the Plan Of Record (POR) for all Intel mobile processors     |
| Passive Trip Point  | 15°C<br>...<br><b>90°C</b><br>95°C | This value controls the temperature of the ACPI Passive Trip Point - the point where the OS begins throttling the processor  |
| - Passive TC1 Value | <b>1</b>                           | This value sets the TC1 value for the ACPI Passive Cooling Formula. Range 1 - 16   |
| - Passive TC2 Value | <b>5</b>                           | This value sets the TC2 value for the ACPI Passive Cooling Formula. Range 1 - 16   |
| - Passive TSP Value | <b>10</b>                          | This item sets the TSP value for the ACPI Passive Cooling Formula. It represents in tenth of a second how often the OS will read the temperature when passive cooling is enabled. Range 2 - 32 |

## Passive Cooling



The ACPI OS assesses the optimum CPU performance change necessary to lower the temperature using the following equation

$$\Delta P[\%] = TC1(T_n - T_{n-1}) + TC2(T_n - T_t)$$

$\Delta P$  is the performance delta,  $T_t$  is the target temperature = passive cooling trip point. The two coefficients  $TC1$  and  $TC2$  and the sampling period  $TSP$  are hardware dependent constants the end user must supply. It's up to the end user to set the cooling preference of the system by setting the appropriate trip points in the BIOS setup.



See chapter 12 of the ACPI specification ([www.acpi.info](http://www.acpi.info)) for more details

## ICC Configuration

| Phoenix SecureCore Technology Setup |                      |  |
|-------------------------------------|----------------------|--|
| Advanced                            |                      |  |
| ICC Configuration                   |                      | Item Specific Help   |
| Use Watchdog Timer for ICC          | [Disabled]           | Enable Watchdog Timer operation for ICC.If enabled,Watchdog Timer will be started after ICC related changed. This timer detects platform instability caused by wrong clock settings. |
| <b>Clock Manipulation</b>           | <b>[ICC Success]</b> |  |
| Apply ICC settings after reboot     | [None]               |  |
| ICC Overclocking Library            | [9.0.0.1209]         |  |
| ▶ Clock 3                           |                      |  |

Esc Exit → Select Menu Enter Select ▶ Sub-Menu F10 Save and Exits

| Feature                         | Options                          | Description   |
|---------------------------------|----------------------------------|---|
| Use Watchdog Timer for ICC      | Disabled<br>Enabled              | Enable Watchdog Timer operation for ICC. If enabled, Watchdog Timer will be started after ICC related changed. This timer detects platform instability caused by wrong clock settings |
| Apply ICC settings after reboot | Permanently after reboot<br>None | None: Change will not apply Permanently: Changes will be applied permanently, starting after the next reboot. Use it to provide changes that are verified and safe.                   |

## Clock 3

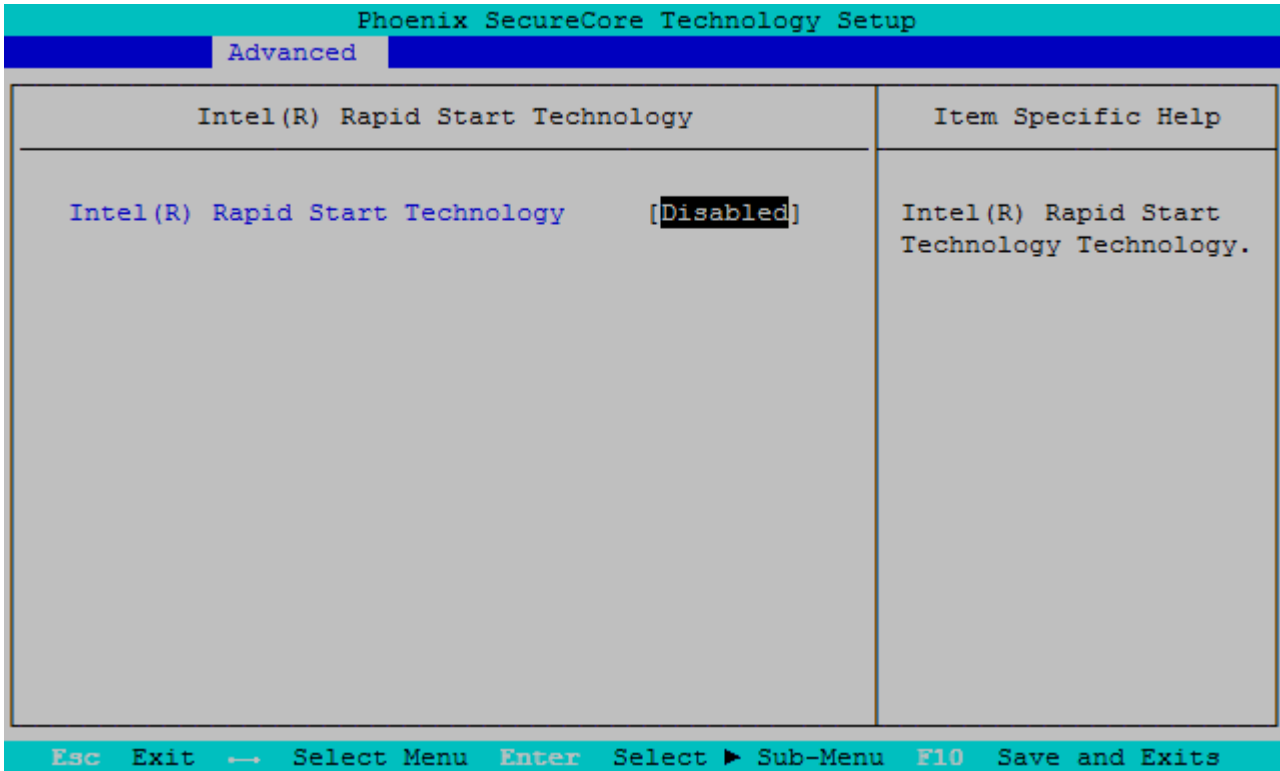
| Phoenix SecureCore Technology Setup       |              |  |
|---|--------------|--|
| Advanced                                  |              |  |
| Clock 3                                   |              | Item Specific Help   |
| BCLK, DMI, PEG, PCIe<br>PCI33, SATA, USB3 |              | Clock spectrum spread in 0.01% increments. Determines spectrum deviation away from base frequency. Allowed range is limited by Max supported SSC%. Changes will not be applied unless 'Apply settings' is pressed. |
| Current frequency                         | [100.0 MHz ] |  |
| Current SSC mode                          | [down]       |  |
| Maximum supported SSC %                   | [0.50 ]      |  |
| Current SSC %                             | [0.50 ]      |  |
| New SSC spread percent                    | [50]         |  |

Esc Exit → Select Menu Enter Select ▶ Sub-Menu F10 Save and Exits

| Feature                | Options | Description   |
|------------------------|---------|---|
| New SSC spread percent | 50      | Clock spectrum spread in <b>0.01%</b> increments. Determines spectrum deviation away from base frequency. Allowed range is limited by Max supported SSC%. |

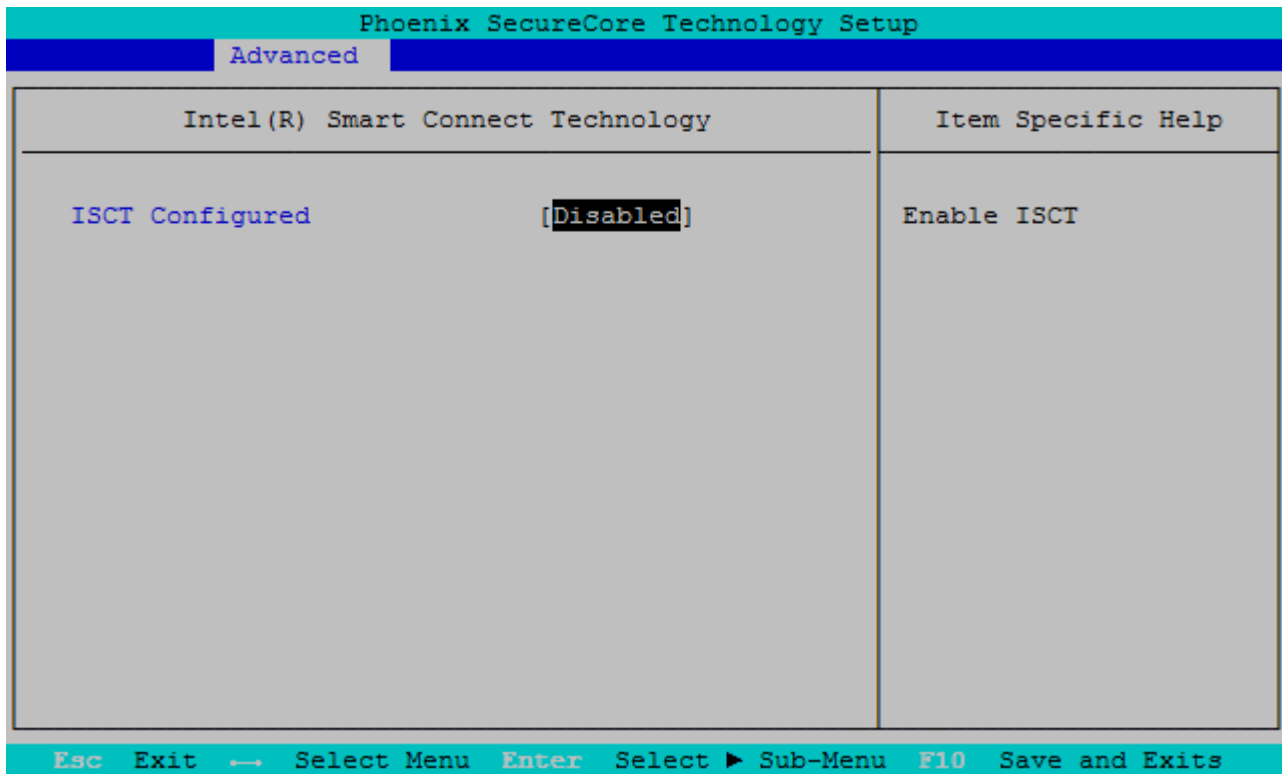


## Intel® Rapid Start Technology



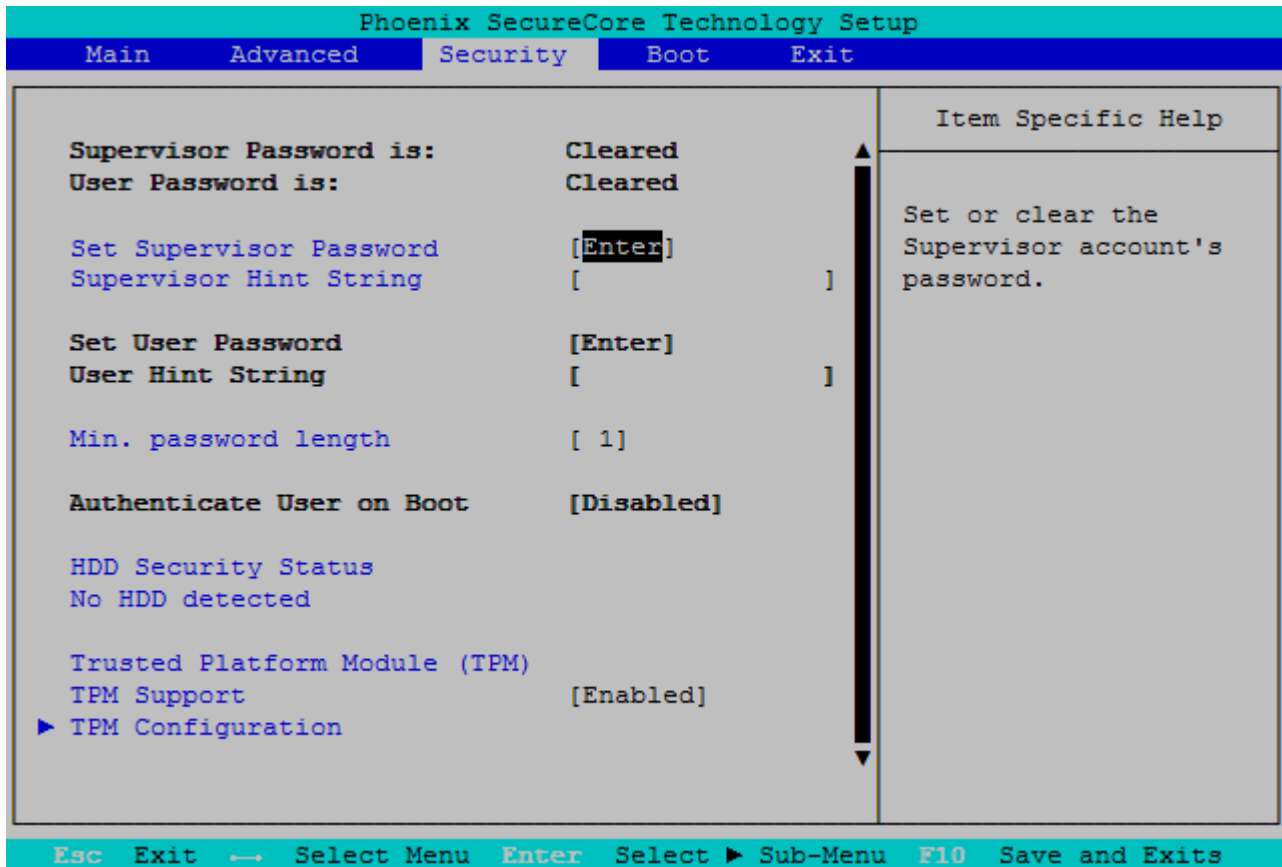
| Feature                                   | Options   | Description   |
|---|---|---|
| Intel® Rapid Start Technology Support     | Disabled<br>Enabled   | Enable/Disable Intel® Rapid Start Technology              |
| - Entry on S3 RTC wake                    | Disabled<br>Enabled   | Intel® Rapid Start Technology invocation upon S3 RTC wake |
| - Entry after                             | Immediately<br>1 minute<br>2 minutes<br>5 minutes<br><b>10 minutes</b><br>15 minutes<br>30 minutes<br>1 hour<br>2 hours | RTC wake timer at S3 entry                                |
| - Display Save Restore                    | Disabled<br>Enabled   | Display Save Restore configuration                        |
| - Intel® Rapid Start Technology Partition | -   | Indicates a valid partition for Rapid Start Support       |

## Intel® Smart Connect Technology



| Feature                   | Options                       | Description   |
|---------------------------|-------------------------------|---|
| ISCT Configured           | Disabled<br>Enabled           | Enable Intel® Smart Connect Technology  |
| ISCT Notification Control | Disabled<br>Enabled           | Enable ISCT Notification Control  |
| ISCT WLAN Power Control   | Disabled<br>Enabled           | Enable ISCT WLAN Power Control  |
| ISCT WWAN Power Control   | Disabled<br>Enabled           | Enable ISCT WWAN Power Control  |
| ISCT SASD Format Control  | Actual Time<br>Sleep Duration | Select ISCT wake time format for ACPI SASD method.<br>Actual Time: -YYMMDDHHMMSS<br>Sleep Duration: - Duration in seconds |

### 8.5.3 Security



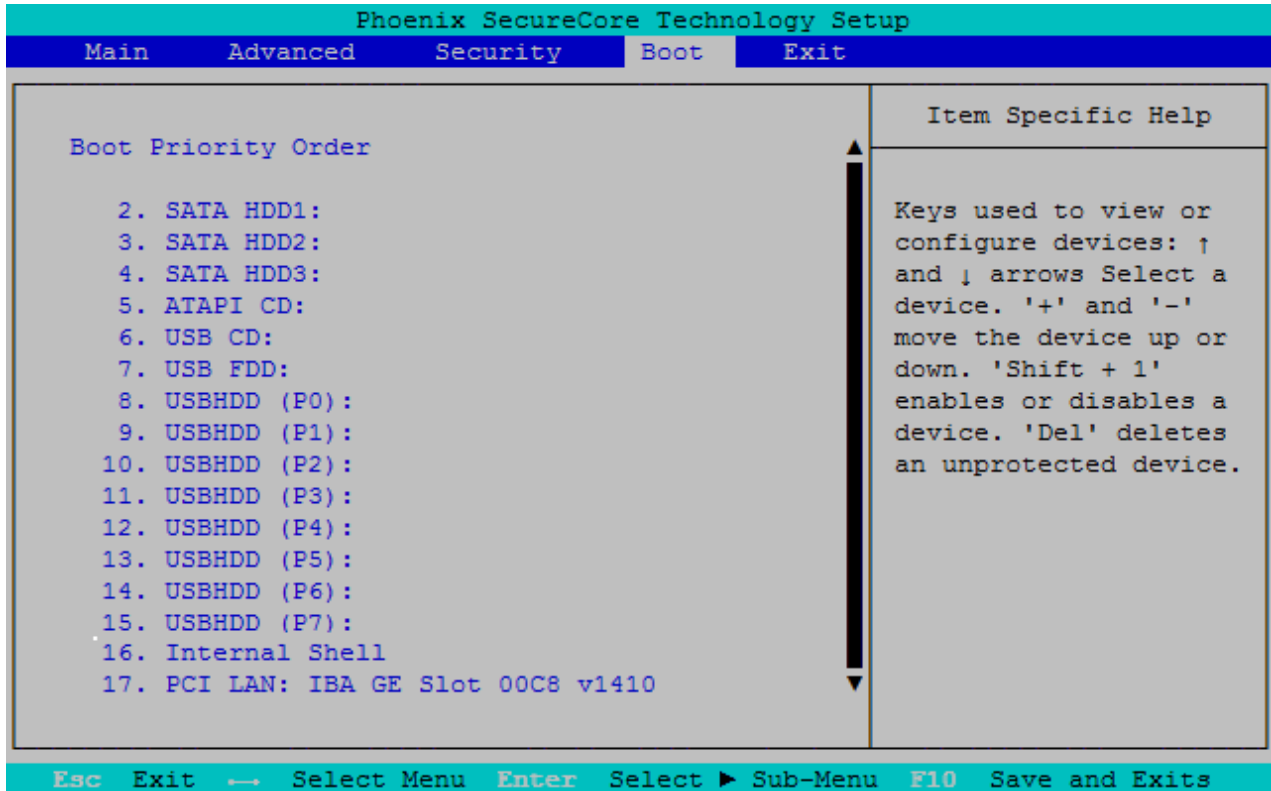
| Feature                 | Options             | Description  |
|-------------------------|---------------------|--|
| Set Supervisor Password | Enter               | Set or clear the Supervisor account's password                           |
| Supervisor Hint String  | -                   | Press Enter to type Supervisor Hint String                               |
| Min. password length    | 1                   | Set the minimum number of characters for password (1-20)                 |
| TPM Support             | Disabled<br>Enabled | This is used to decide whether TPM support should be enabled or disabled |

## Security

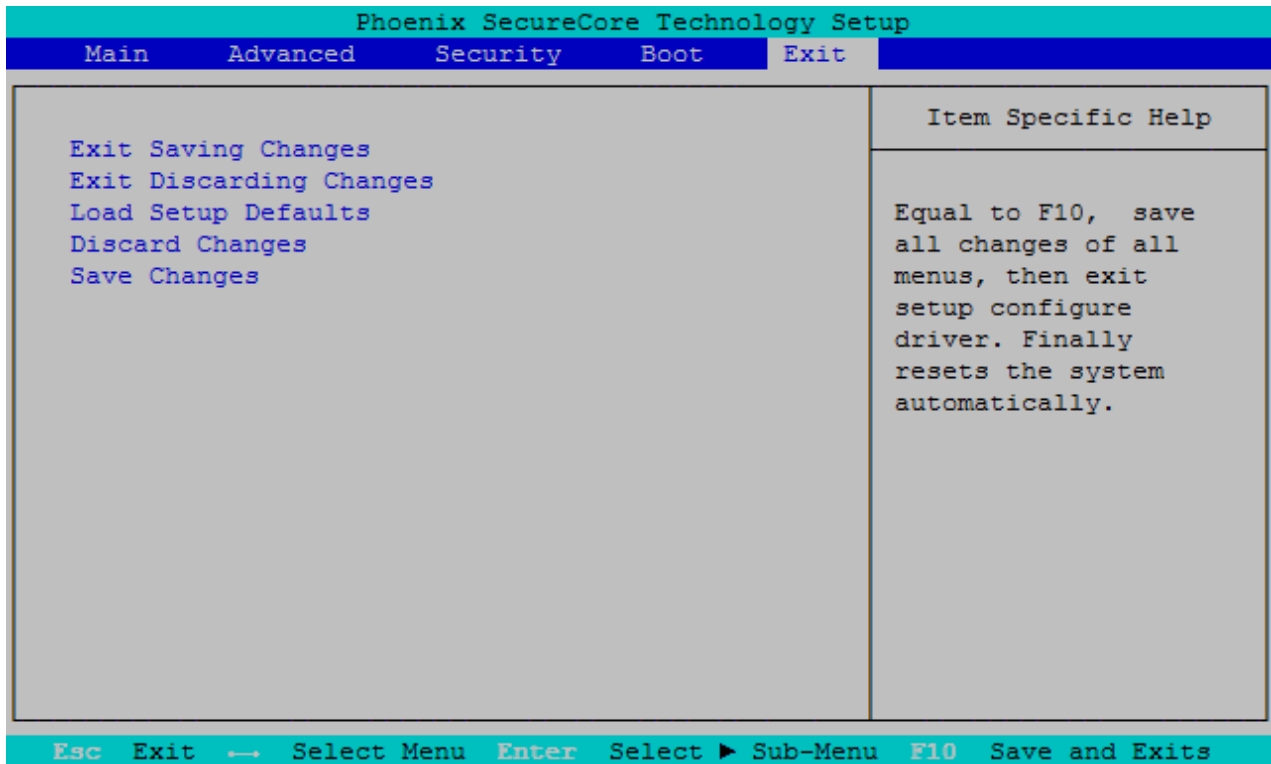
| Phoenix SecureCore Technology Setup  |  |
|--|--|
| Security   |  |
| TPM Configuration  | Item Specific Help   |
| <p>Current TPM State      <b>[Enabled and Activated]</b><br/>           TPM Action            [No Change]<br/>           Omit Boot Measurements [Disabled]</p> | <p>Enact TPM Action.<br/>           Note: Most TPM actions require TPM to be Enabled to take effect.</p> |
| <p>Esc Exit   ← Select Menu   Enter Select ▶ Sub-Menu   F10 Save and Exits</p>   |  |

| Feature                | Options   | Description   |
|------------------------|---|---|
| TPM Action             | <b>No Change</b><br>Enable<br>Disable<br>Activate<br>Deactivate<br>Clear<br>Enable and Activate<br>Disable and Deactivate<br>Set Owner Install, with state=True<br>Set Owner Install, with state=False<br>Enable, Activate, and Set Owner Install with state=True<br>Disable, Deactivate, and Set Owner Install with state=False<br>Clear, Enable, and Activate<br>Require PP for provisioning<br>Do not require PP for provisioning<br>Require PP for clear<br>Do not require PP for clear<br>Enable, Activate, and clear<br>Enable, Activate, Clear, Enable, and Activate | Enact TPM Action  |
| Omit Boot Measurements | Disabled<br><b>Enabled</b>  | Enabling this option causes the system to omit recording boot device attempts in PCR[4] |

## 8.5.4 Boot



## 8.5.5 Exit



## Corporate Offices

**Global Headquarters**

Kontron S&T AG  
Lise-Meitner-Str. 3-5  
86156 Augsburg  
Germany  
Tel.: +49 821 4086-0  
Fax: +49 821 4086-111

