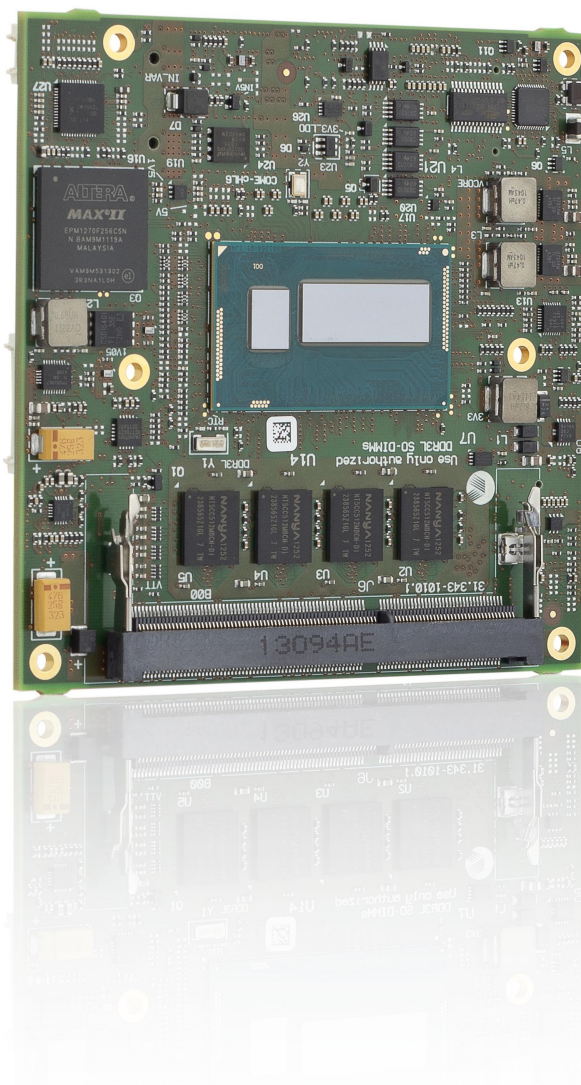


» Kontron User's Guide «



COMe-cHL6

Document Revision 110

» Table of Contents «

1	<u>User Information</u>	5
1.1	<u>About This Document</u>	5
1.2	<u>Copyright Notice</u>	5
1.3	<u>Trademarks</u>	5
1.4	<u>Standards</u>	5
1.5	<u>Warranty</u>	6
1.6	<u>Technical Support</u>	6
2	<u>Introduction</u>	7
2.1	<u>Product Description</u>	7
2.2	<u>Naming clarification</u>	8
2.3	<u>Understanding COM Express® Functionality</u>	8
2.4	<u>COM Express® Documentation</u>	9
2.5	<u>COM Express® Benefits</u>	9
3	<u>Product Specification</u>	10
3.1	<u>Module definition</u>	10
3.2	<u>Functional Specification</u>	11
3.3	<u>Block Diagram</u>	18
3.4	<u>Accessories</u>	19
3.5	<u>Electrical Specification</u>	20
3.5.1	<u>Supply Voltage</u>	20
3.5.2	<u>Power Supply Rise Time</u>	20
3.5.3	<u>Supply Voltage Ripple</u>	20
3.5.4	<u>Power Consumption</u>	20
3.5.5	<u>ATX Mode</u>	21
3.5.6	<u>Single Supply Mode</u>	21
3.6	<u>Power Control</u>	22
3.7	<u>Environmental Specification</u>	23
3.7.1	<u>Temperature Specification</u>	23
3.7.2	<u>Humidity</u>	23
3.8	<u>Standards and Certifications</u>	24
3.9	<u>MTBF</u>	26
3.10	<u>Mechanical Specification</u>	27
3.11	<u>Module Dimensions</u>	28
3.12	<u>Thermal Management, Heatspreader and Cooling Solutions</u>	29
4	<u>Features and Interfaces</u>	30
4.1	<u>S5 Eco Mode</u>	30
4.2	<u>LPC</u>	31
4.3	<u>Serial Peripheral Interface (SPI)</u>	32
4.4	<u>SPI boot</u>	32

4.5	M.A.R.S.	34
4.6	UART	35
4.7	Fast I2C	36
4.8	Dual Staged Watchdog Timer	37
4.9	Intel® Fast Flash Standby™ / Rapid Start Technology™	38
4.10	Speedstep Technology	40
4.11	C-States	41
4.12	Hyper Threading	42
4.13	Intel® Turbo Boost Technology and AVX	43
4.14	Display Configuration	44
4.15	Hybrid Graphics / Multi-monitor	47
4.16	Intel® vPro™ technology	48
4.17	ACPI Suspend Modes and Resume Events	49
5	System Resources	50
5.1	Interrupt Request (IRQ) Lines	50
5.2	Memory Area	51
5.3	I/O Address Map	51
5.4	Peripheral Component Interconnect (PCI) Devices	52
5.5	Internal I2C Bus	52
5.6	External I2C Bus	52
5.7	System Management (SM) Bus	53
6	Connectors	54
6.1	Connector Location	54
7	Pinout List	55
7.1	General Signal Description	55
7.2	Connector X1A Row A	56
7.3	Connector X1A Row B	58
7.4	Connector X1B Row C	60
7.5	Connector X1B Row D	62
8	BIOS Operation	64
8.1	Determining the BIOS Version	64
8.2	BIOS Update	64
8.3	POST Codes	64
8.4	Setup Guide	65
8.5	BIOS Setup	66
8.5.1	Main	66
8.5.2	Advanced	72
8.5.3	Security	109
8.5.4	Boot	111
8.5.5	Exit	112

1 User Information

1.1 About This Document

This document provides information about products from Kontron Europe GmbH and/or its subsidiaries. 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.

1.2 Copyright Notice

Copyright © 2003-2014 Kontron Europe GmbH

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 Europe GmbH.

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

1.3 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.

1.4 Standards

Kontron Europe GmbH is certified to ISO 9000 standards.

1.5 Warranty

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

1.6 Technical Support

Technicians and engineers from Kontron Europe GmbH 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

Tailored for most robust and maintenance-free system designs in the high performance class of embedded systems

Kontron is extending the usage model of the 4th generation Intel® Core® processor technology to compact and rugged fanless options with the launch of the Kontron COMe-cHL6 COM Express® compact Computer-on-Modules. The new modules in the compact form factor (95 x 95 mm) are equipped with the ULT versions of the 4th generation Intel® Core™ i7/i5/i3 & Celeron® processor, formerly codenamed 'Haswell-U'. ULT stands for ultra-low TDP which limits the power consumption of these new Computer-on-Modules down to options that are tailored for fanless and fully enclosed system designs. The modules also cater for the most robust and maintenance-free system designs in the high performance class of embedded systems, and consequently help engineers to reduce the systems' bill of materials as well as the customers' total cost of ownership.

Application areas can be found in all the performance-hungry but power-restricted, multi-touch multi-display systems such as HMIs in automation, medical imaging, digital signage and point of sale as well as surveillance and security. The modules also address the fast-growing, industrial-grade tablet PC market for various industries including logistics, retail and manufacturing.

The Kontron COMe-cHL6 COM Express® compact Computer-on-Modules with pin-out type 6 are highly scalable to cover a broad application range from high-end 1.7 GHz dual-core Intel® Core™ i7 processor performance to cost-optimized Intel® Celeron® designs. With Intel® AVX2 and OpenCL 1.2 they boost floating point performance as well as parallel processing density. Up to 16 GB of energy-efficient DDR3L RAM (8GB memory down + 8GB SODIMM) satisfy even highest memory demands. State-of-the-art multi-display designs are enabled by three independent display outputs, executed via 2x DP++ (DisplayPort, HDMI, DVI) and 1x Dual Channel LVDS. Standard interfaces include 4x SATA 6Gbit/s ports, Gigabit Ethernet, 2x USB 3.0 ports and 8x USB 2.0. Application-specific extensions on the carrier board are connected via 4x PCIe x1 or 1x PCI x4. An additional PCIe x2 interface is possible with disabled GbE functionality. The wide-range (8.5 - 20V) power supply and MARS smart battery support simplify mobile and battery-powered designs.

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-cHL6. 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® compact sized Computer-on-Module COMe-chL6 (CHL6) follows pin-out Type 6 and is compatible to PICMG specification COM.0 Rev 2.1. The COMe-chL6 based on latest Shark Bay ULT 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	Memory Down	SATA
36014-4000-17-7	COMe-chL6 i7-4650U 4GB	Intel® Core™ i7-4650U	4GB	4x 6Gb/s
36014-0000-17-7	COMe-chL6 i7-4650U	Intel® Core™ i7-4650U	-	4x 6Gb/s
36014-4000-19-5	COMe-chL6 i5-4300U 4GB	Intel® Core™ i5-4300U	4GB	4x 6Gb/s
36014-0000-19-5	COMe-chL6 i5-4300U	Intel® Core™ i5-4300U	-	4x 6Gb/s
36014-4000-17-3	COMe-chL6 i3-4010U 4GB	Intel® Core™ i3-4010U	4GB	4x 6Gb/s
36014-0000-17-3	COMe-chL6 i3-4010U	Intel® Core™ i3-4010U	-	4x 6Gb/s
36014-0000-16-1	COMe-chL6 2980U	Intel® Celeron 2980U	-	2x 6Gb/s

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

The COMe-chL6 is available for extended temperature grade on request. General capability was tested for following options:

- » CPU: all
- » Memory: all DDR3L
- » VCC: 12V only, no support for Wide-Range Input

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

Modules for E2 temperature range are available project based only, please contact your local sales or support for further details. General capability was tested for following options:

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

3.2 Functional Specification

Processor

The 22nm Intel® 4th Gen Core™ i7/i5/i3/Celeron® embedded (Haswell-U (ULT)) CPU family with 40x24mm package size (BGA1168 socket) supports:

- » Intel® Turbo Boost Technology 2.01
- » Intel® 64
- » Intel® Virtualization Technology (VT-x)
- » Intel® Virtualization Technology for Directed I/O (VT-d)
- » AES New Instructions (AES-NI)
- » 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
- » Configurable Thermal Design Power (cTDP)
- » Intel® Rapid Storage Technology
- » Intel® Smart Connect Technology

Optional available (with customized BIOS):

- » 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 xxxx supports:

- » GraphicsTechnology GT2 with 20 Execution Units or GT3 with 40 Execution Units
- » 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

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

Intel®	Core™	Core™	Core™	Core™
-	i7-4650U	i5-4300U	i3-4010U	Celeron 2980U
# of Cores	2	2	2	2
# of Threads	4	4	4	2
TDP Core frequency (HFM)	1700MHz	1900MHz	1700MHz	1600MHz
Max Turbo Frequency 1 core	3300MHz	2900MHz	-	-
Max Turbo all cores	2900MHz	2500MHz	-	-
LFM/LPM Frequency	800MHz	800MHz	800MHz	800MHz
Bus/Core Ratio	8 - 17	8 - 19	8 - 17	8 - 16
TjMax	100°C	100°C	100°C	100°C
Thermal Design Power (TDP)	15W	15W	15W	15W
cTDP-Down	11.5W (800MHz)	11.5W (800MHz)	11.5W (800MHz)	-
cTDP-Up	25W (2.3GHz)	25W (2.5GHz)	-	-
Power Limit 2 (PL2 max)	31.25W	31.25W	25W	18.75W
C-States	C0-C10	C0-C10	C0-C10	C0-C3
Smart Cache	4MB	3MB	3MB	2MB
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	8+4GB	8+4GB	8+4GB	8+4GB
# of Memory Channels	2	2	2	2
Graphics Model	HD5000	HD4400	HD4400	HD
GFX Base Frequency	200MHz	200MHz	200MHz	200MHz
GFX Max Dynamic Frequ.	1100MHz	1100MHz	1000MHz	1000MHz
GFX Technology	GT3 40EU	GT2 20EU	GT2 20EU	GT1 10EU
Quick Sync Video	Yes	Yes	Yes	-
InTru™ 3D	Yes	Yes	Yes	-
Wireless Display	Yes	Yes	Yes	-
Clear Video HD	Yes	Yes	Yes	-
vPRO™ (optional)	Yes	Yes	-	-
TXT (optional)	Yes	Yes	-	-
AES-NI (optional)	Yes	Yes	Yes	-
VT-x	Yes	Yes	Yes	Yes
VT-d	Yes	Yes	Yes	-
PCI Express Graphics x16	-	-	-	-

Memory

Sockets	1x DDR3L SODIMM, 1x memory down
Memory Type	DDR3L-1600
Maximum Size	1-8GB SODIMM, 2-4GB memory down
Technology	Dual Channel

Chipset

The integrated Intel® Platform Controller Hub LynxPoint-LP 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

HighSpeed I/O Port Configuration

Internal	Port Usage	COMe
Port1	USB3 #1	USB #0 = USB3.0
Port2	USB3 #2	USB #1 = USB3.0
Port3	PCIe #1 or USB3 #3	PCIe #0
Port4	PCIe #2 or USB3 #4	PCIe #1
Port5	PCIe #3	PCIe #2
Port6	PCIe #4	PCIe #3
Port7	PCIe #5L0	PCIe #4
Port8	PCIe #5L1	PCIe #5 (x2 only with #4)
Port9	PCIe #5L2	Ethernet (PCIe #6 w/o LAN)
Port10	PCIe #5L3	not used (PCIe #7 w/o LAN)
Port11	PCIe #6L0 or SATA6 #3	SATA #3 (6Gbps)
Port12	PCIe #6L1 or SATA6 #2	SATA #2 (6Gbps)
Port13	PCIe #6L2 or SATA6 #1	SATA #1 (6Gbps)
Port14	PCIe #6L3 or SATA6 #0	SATA #0 (6Gbps)



x2 Port PCIe #4 + #5 are only available with Softstrap option (modified Flash descriptor) which disables onboard LAN (PCIe #5L2)

Graphics Core

The integrated Intel® HD/HD4400/HD5000 (Gen7.5) supports:

Graphics Core Render Clock	GT1/GT2; Base clock: 200 MHz; GT Turbo: up to 1100 MHz
Execution Units / Pixel Pipelines	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	-
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	-
Digital Display Interface DDI1	DP++
Digital Display Interface DDI2	DP++
Digital Display Interface DDI3	-
Maximum Resolution on DDI	HDMI: 4096x2304, DP: 3200x2000

Storage

onboard SSD	-
SD Card support	-
IDE Interface	-
Serial-ATA	4x SATA 6Gb/s
SATA AHCI	AHCI with NCQ, HotPlug, Staggered Spinup, eSATA, PortMultiplier
SATA RAID	0, 1, 5, 10



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 enable RAID support in BIOS Chipset/SATA settings, connect at least two hard drives and enter the RAID Option ROM by pressing 'CTRL'+ 'I'

Connectivity

USB 2.0	8x USB 2.0
USB 3.0	2x USB 3.0
USB Client	-
PCI	-
PCI External Masters	-
PCI Express	4x PCIe x1 Gen2
Max PCI Express	8x PCIe w/o LAN
PCI Express x2/x4 configuration	YES (Softstrap option)
Ethernet	10/100/1000 Mbit
Ethernet controller	Intel® i218-LM (Clarkville)



Due to internal chipset configuration the LynxPoint-LP only supports up to 4 USB Hubs

PCI Express Configuration

By default, the COMe-CHL6 supports x1 PCIexpress lane configuration only (Configuration 0). Following x2/x4 configurations are available via Management Engine Softstrap Options with a customized Flash Descriptor.

COMe PCIe	Port #0	Port #1	Port #2	Port #3	Port #4	Port #5	Port #6	Port #7
Configuration0	x1	x1	x1	x1	-	-	-	-
Configuration1	x1	x1	x1	x1	x1	-	-	-
Configuration2	x2		x1	x1	-	-	-	-
Configuration3	x2		x2		x2		-	-
Configuration4	x2		x1	x1	x2		-	-
Configuration5	x4				x4			



Configuration0 is default setting. Other configurations are available via modified FlashDescriptor with customized BIOS versions. For configurations 2 to 5 the onboard Ethernet will be disabled.

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
Miscellaneous	2x UART / PWM FAN / optional eDP

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/i5/i3

Power Consumption and Performance

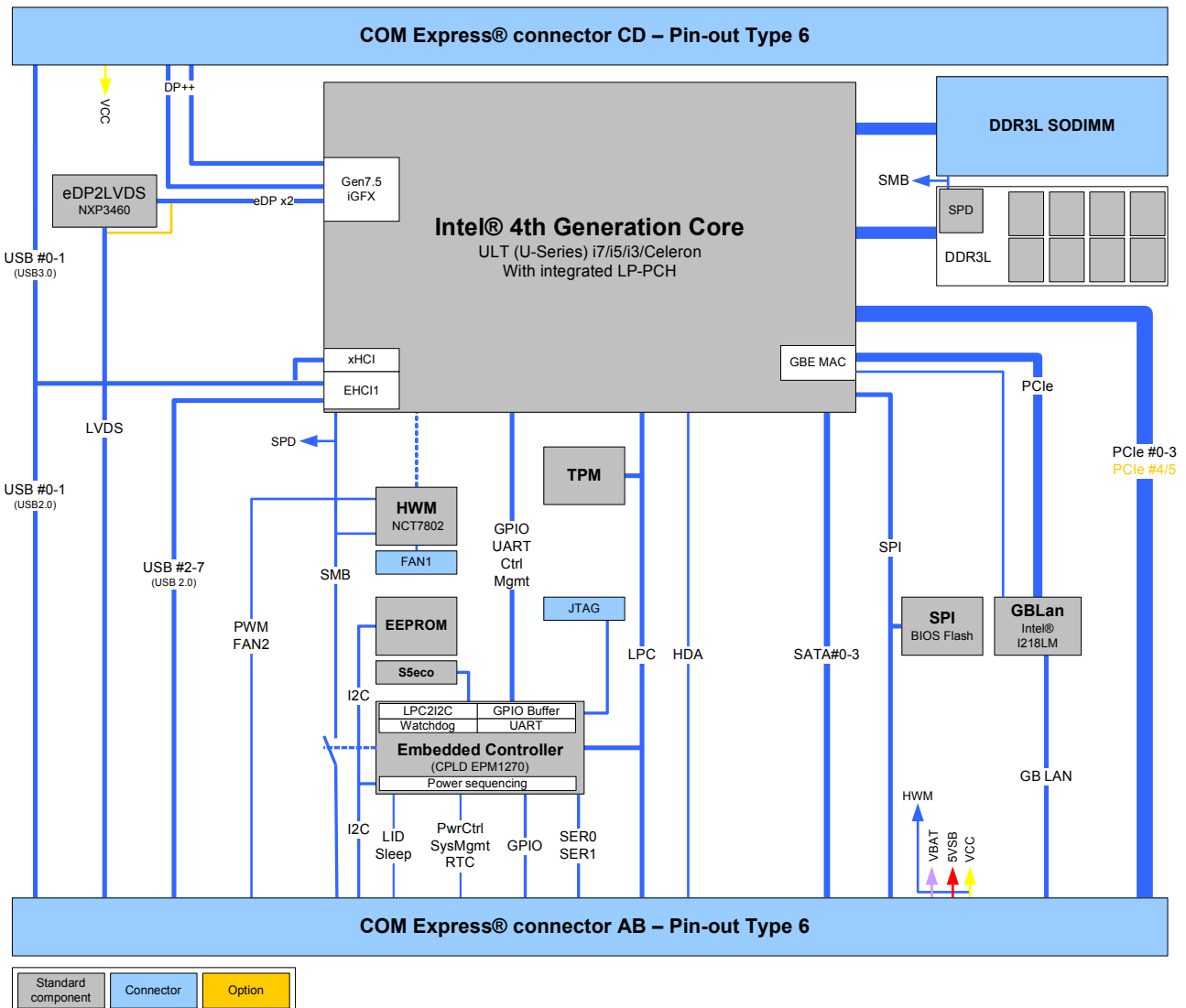
Full Load Power Consumption	14 - 30W
Kontron Performance Index	41000 - 65269
Kontron Performance/Watt	2009 - 2997

*Measured Values. Please note the maximum Power Consumption with activated Turbo Mode in chapter Turbo 2.0



Detailed Power Consumption measurements in all states and benchmarks for CPU, Graphics and Memory performance 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
36014-0000-99-0	HSP COMe-cHL6 thread	For all CPUs and temperature grades
36014-0000-99-1	HSP COMe-cHL6 through	For all CPUs and temperature grades

General accessories

Part Number	COMe pin-out Type 6 compatible accessories	Project Code	Comment
38114-0000-00-0	COM Express® Reference Carrier Type 6	ADAS	mITX Carrier with 8mm COMe connector
38106-0000-00-0	COM Express® Eval Carrier Type 6	Topanga Canyon	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
38106-0000-00-5	COMe Eval Starterkit T6	Topanga Canyon	Starterkit with COMe Evaluation Carrier T6
38114-0000-00-5	COMe Ref. Starterkit T6	ADAS	Starterkit with COMe Reference Carrier T6
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	
9-5000-0352	ADA-LVDS-DVI 18bit	LVDS to DVI converter	
9-5000-0353	ADA-LVDS-DVI 24bit	LVDS to DVI converter	
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	
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		

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-CHL6 variants is 14 - 30W (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-cHL6 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-cHL6 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-CHL6

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 Screening (XT)	-40°C to +85°C	-40°C to +85°C	VCC: 12V
Industrial grade by Design (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 Screening (XT)	at 85°C HSP temperature the CPU @ 50% load is allowed to start throttling for thermal protection
Industrial grade by Design (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-cHL6** 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® compact** 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® compact** 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-cHL6** 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): 342363 @ 40°C (w/PCB)



Fans usually shipped with Kontron Europe GmbH 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 95.0 mm (3.75" x 3.75")

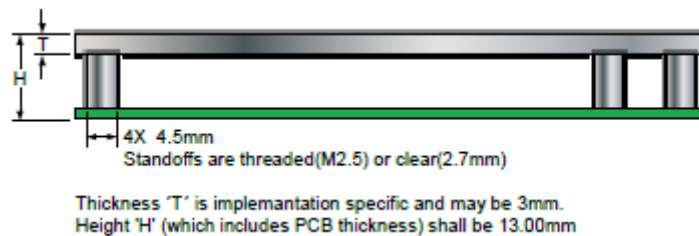
» Height approx. 12mm (0.4")



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

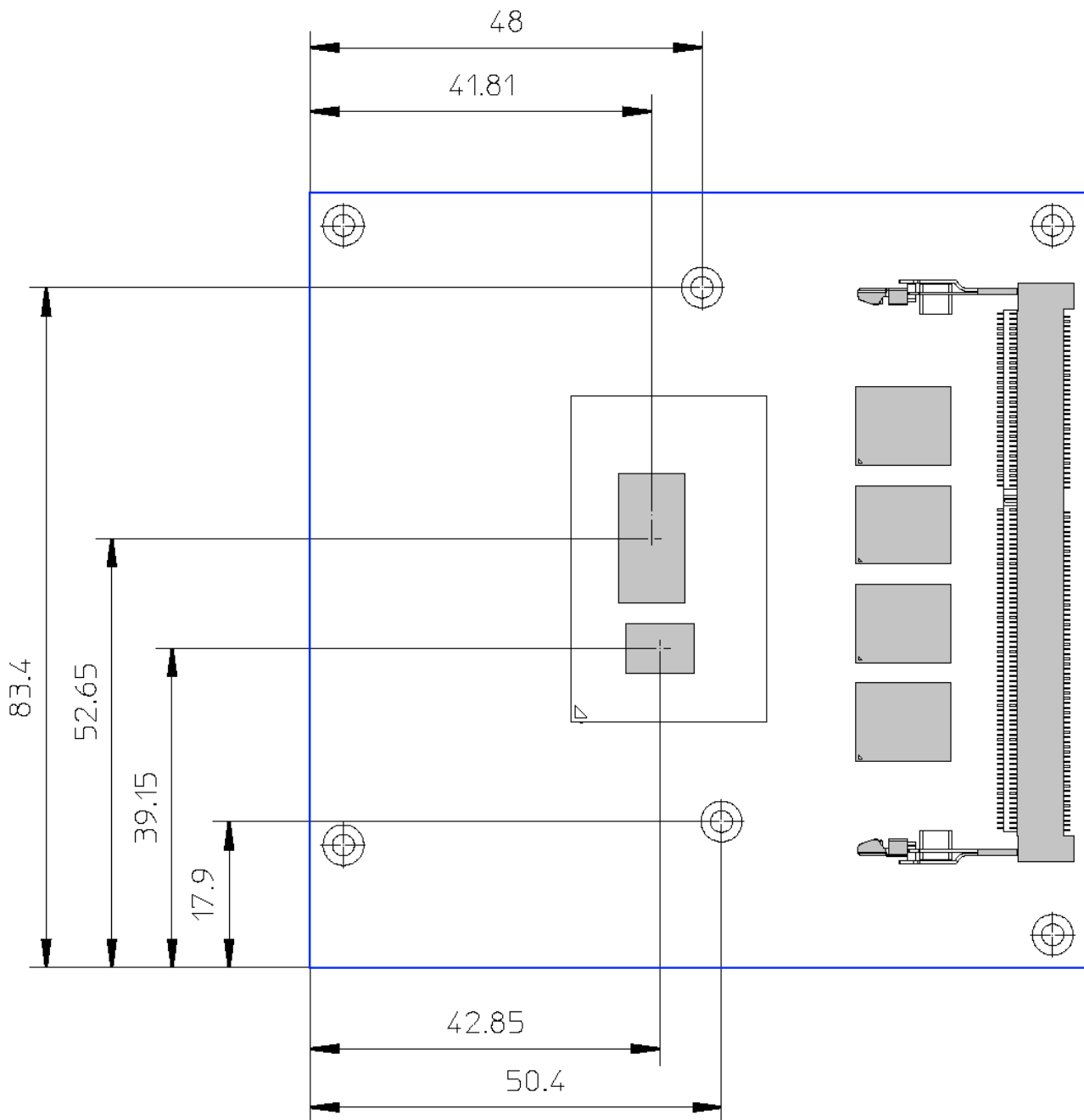
Height

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



Cooling solutions provided from Kontron Europe GmbH for compact 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



All dimensions in mm

3.12 Thermal Management, Heatspreader and Cooling Solutions

A heatspreader plate assembly is available from Kontron Europe GmbH for the COMe-cHL6. 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-cHL6. 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 Europe GmbH for the COMe-cHL6 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-cHL6 heatspreader and cooling solutions are provided at <http://emdcustomersection.kontron.com>.

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 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.

4.3 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.

4.4 SPI boot

The COMe-chL6 supports boot from an external SPI Flash. It can be configured by pin A34 (BIOS_DIS#0) and pin B88 (BIOS_DIS#1) 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	Manufacturer	Part Number	Device ID
16Mbit	Atmel	AT26DF161	0x1F4600
16Mbit	Atmel	AT26DF161A	0x1F4601
16Mbit	Atmel	AT25DF161	0x1F4602
16Mbit	Atmel	AT25DQ161	0x1F8600
16Mbit	Macronix	MX25L1605A(D)(36E)(06E)	0xC22015
16Mbit	Macronix	MX25L1635D	0xC22415
16Mbit	SST/Microchip	SST25VF016B	0xBF2541
16Mbit	Winbond	W25X16BV	0xEF3015
16Mbit	Winbond	W25Q16BV(CV)	0xEF4015
Size	Manufacturer	Part Number	Device ID
32Mbit	Atmel	AT25/26DF321	0x1F4700
32Mbit	Atmel	AT25DF321A	0x1F4701
32Mbit	Macronix	MX25L3205A(D)(06E)	0xC22016
32Mbit	Macronix	MX25L3225D(35D)(36D)	0xC25E16
32Mbit	SST/Microchip	SST25VF032B	0xBF254A
32Mbit	Winbond	W25X32BV	0xEF3016
32Mbit	Winbond	W25Q32BV,	0xEF4016
Size	Manufacturer	Part Number	Device ID
64Mbit	Atmel	AT25DF641(A)	0x1F4800
64Mbit	Atmel	AT25DQ641	0x1F8800
64Mbit	Macronix	MX25L6405D(45E)(36E)(06E)(73E)	0xC22017
64Mbit	Macronix	MX25L6455E	0xC22617
64Mbit	Macronix	MX25U6435F	0xC22537
64Mbit	SST/Microchip	SST25VF064C	0xBF254B
64Mbit	Winbond	W25X64BV	0xEF3017
64Mbit	Winbond	W25Q64BV(CV)(FV)	0xEF4017
64Mbit	Winbond	W25Q64DW	0XEF6017
64Mbit	Winbond	W25Q64FW	0XEF6017

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.

4.5 M.A.R.S.

The Smart Battery implementation for Kontron Computer-on-Modules called **M**obile **A**pplication for **R**echargeable **S**ystems 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

4.6 UART

The COMe-cHL6 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.

4.7 Fast I2C

The COMe-cHL6 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

4.8 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-CHL6 offers a watchdog which works with two stages that can be programmed independently and used one by one.

Time-out events

Reset	A reset will restart the module and starts POST and operating system new.
NMI	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.
SCI	A system control interrupt (SCI) is a OS-visible interrupt to be handled by the OS using AML code
Delay	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)
WDT Signal only	This setting triggers the WDT Pin on baseboard connector (COM Express® Pin B27) only
Cascade:	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.

4.9 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

4.10 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.

4.11 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.

4.12 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.

4.13 Intel® Turbo Boost Technology and AVX

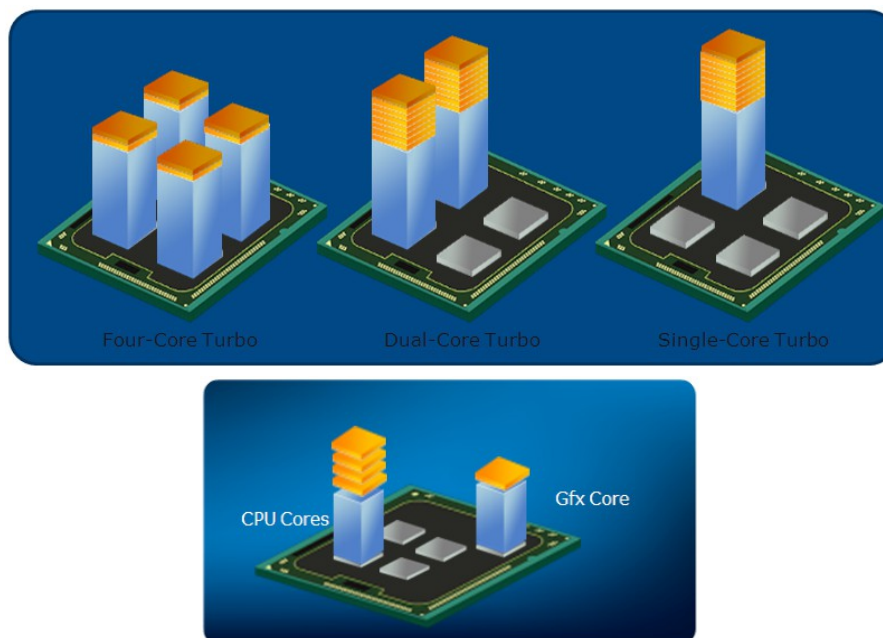
For applications that are particularly power-hungry, the new processors provide enhanced Intel® Turbo Boost technology. This automatically shifts processor cores and processor graphics resources to accelerate performance, tailoring a workload to give users an immediate performance boost for their applications 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.

4.14 Display Configuration

Maximum supported Resolutions in Single Display Configuration

Port	Max Resolution
DP	3200×2000@60Hz, 24bpp
HDMI	4096×2160@24Hz, 24bpp 2560×1600@60Hz, 24bpp 1920×1080@60Hz, 36bpp
DVI	1920×1200@60Hz, 24bpp
WiDi	1920×1080@30Hz, 24bpp 1280×720@60Hz, 24bpp
eDP (x4)	3200×2000@60Hz, 24bpp
LVDS	1920×1200@60Hz

Maximum supported Pixel Clock

Port	Max Pixel Clock
DP	414.5 MHz
HDMI	300 MHz
DVI	165 MHz

DDI supported resolutions

Display1	Display2	Display3	Max.Res Display 1	Max.Res Display 2	Max.Res Display 3
HDMI/DP	HDMI/DP	eDP/LVDS	4096×2160@24Hz 3200×2000@60Hz	4096×2160@24Hz 3200×2000@60Hz	3200×2000@60Hz @ eDP 1920×1200 @ LVDS
DVI	DVI/WiDi	eDP/LVDS	1920×1200@60Hz	1920×1200@60Hz 1920×1080@30Hz	3200×2000@60Hz @ eDP 1920×1200 @ LVDS
DP/HDMI	DVI/WiDi	eDP/LVDS	3200×2000@24Hz 4096×2160@24Hz	1920×1200@60Hz 1920×1080@30Hz	3200×2000@60Hz @ eDP 1920×1200 @ LVDS

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

(valid for 60Hz refresh rate and 24bpp)

3 independent Display Support

The COMe-CHL6 supports up to 3 independent displays in Windows 7/8 and Linux

Digital Display Interface Features

The integrated Intel® HD/HD4400/HD5000 (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:

- » 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.

4.15 Hybrid Graphics / Multi-monitor

The COMe-cHL6 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](#)

4.16 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

4.17 ACPI Suspend Modes and Resume Events

The COMe-cHL6 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/SD Controller	Note(4)	external SIO LPT/SD Controller
6	COM3	Note(4)	external SIO COM1
7	COM4	Note(4)	external SIO COM1
8	RTC	No	-
9	ACPI	No	-
10	-	Yes	-
11	-	Yes	-
12	PS/2 Mouse	Note(4)	external SIO
13	-	Yes	-
14	-	Yes	-
15	-	Yes	-
16	LNK A	No	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; Note(3)
18	LNK C	No	PCIe RP 2 + 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
D0000h – DFFFFh	-	Yes	Free for shadow RAM in standard configurations.
E0000h – FFFFFh	System BIOS	No	Fixed
E0000000h–FEAFFFFFFh	PCIe/IGFX	No	Fixed
FEC00000 – FECFFFFFF	IOAPIC/PCIe	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 Ressources	No	Fixed
0020 – 002D	Interrupt Controller	No	Fixed
002E – 002F	LPC SIO	No	Fixed
0030 – 003D	Interrupt Controller	No	Fixed
0040 – 0042	Timer, Counter	No	Fixed
0043	Reserved	No	Fixed
004E – 004F	LPC SIO	No	Fixed
0050 – 0052	Timer, Counter	No	Fixed
0053	Reserved	No	Fixed
0060 – 006F	Micro-, NMI controller	No	Fixed
0070	Reserved	No	Fixed
0071 – 0077	RTC Controller	No	Fixed
0080	BIOS Postcode	No	Fixed
0081 – 009F	Reserved	No	Fixed
00A0 – 00BD	Interrupt Controller	No	Fixed
00C0 – 00DF	Reserved	No	Fixed
00F0	Interrupt Controller	No	Fixed
0170 – 01F7	Sata Controller	No	Fixed
0200 – 020F	Game Port (LPC)	No	Fixed
0376	Sata Controller	No	Fixed
03F6	Sata Controller	No	Fixed
04D0 – 04D1	Interrupt Controller	No	Fixed
0CF9	Reset Generator	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
1000 – 13FF	Chipset, GPIO	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	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
EHCI1	0:29:0	LNK H	internal	Chipset
LPC Bridge	0:31:0	LNK F	internal	Chipset
SATA	0:31:2	LNK D	internal	Chipset
SMBus	0:31:3	LNK C	internal	Chipset

5.5 Internal I2C Bus

8-bit Address	7-bit Address	Used For	Available	Comment
58h	0x2C	S5 Eco	No	S5 Eco Resistor
A0h	0x50	JILI-EEPROM	No	external LVDS EEPROM for JILI Data
C0h	0x60	LVDS bridge	No	DP to LVDS Bridge

5.6 External I2C Bus

8-bit Address	7-bit Address	Used For	Available	Comment
A0h	0x50	JIDA-EEPROM	No	Module EEPROM
AEh	0x57	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 adress 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
5Ch	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

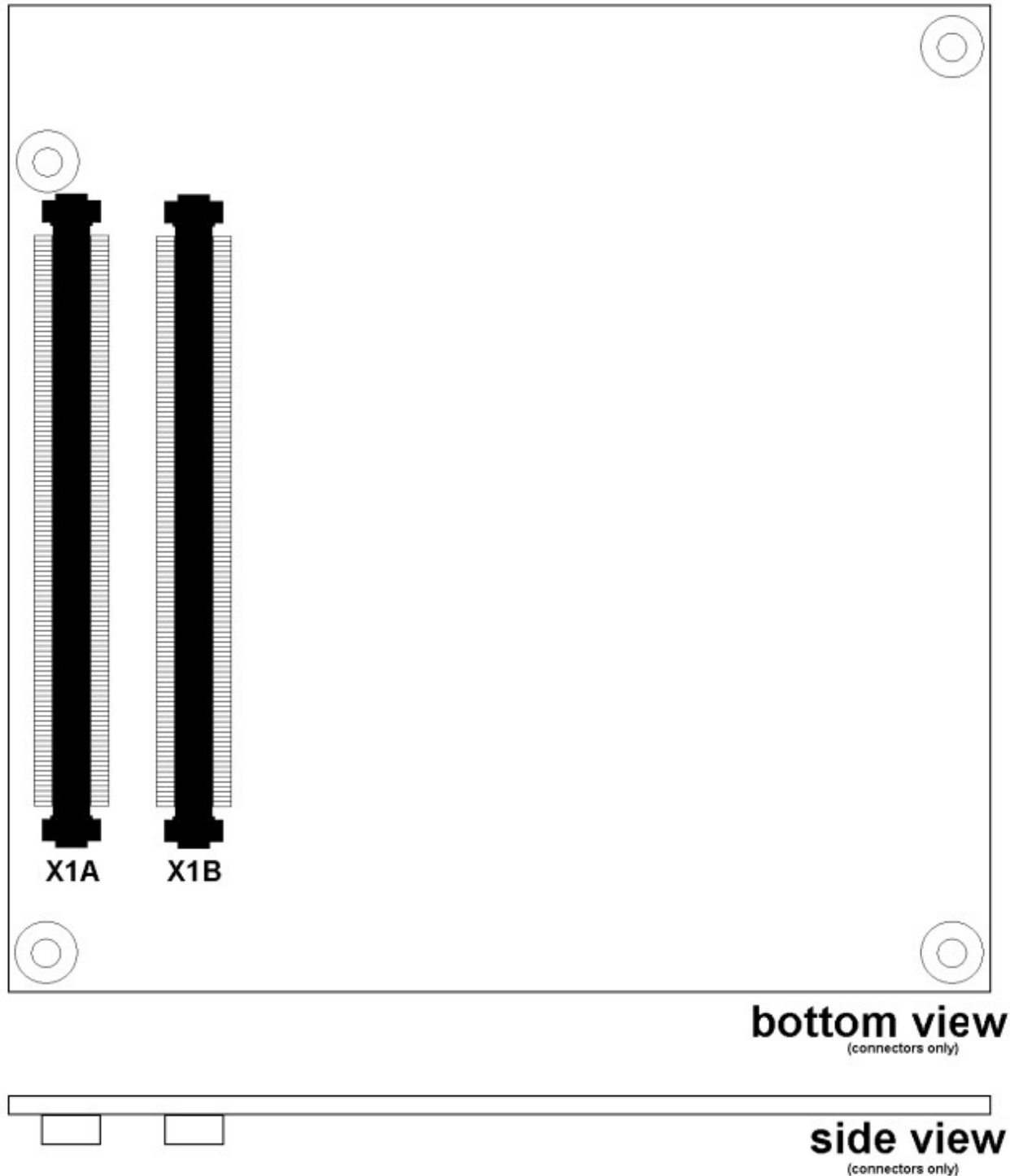


A JIDA Bus No. like in former Modules cannot be provided because the EAPI driver implementation enumerates the I2C busses dynamically. Please follow the initialisation process like it is provided in the EAPI specification.

6 Connectors

The pinouts 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 VIO-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	-	-
A2	GBEO_MDI3-	GBEO_MDI3_N / Ethernet Receive Data -	DP-I	-	-
A3	GBEO_MDI3+	GBEO_MDI3_P / Ethernet Receive Data -	DP-I	-	-
A4	GBEO_LINK100#	GBEO_LINK100# / Ethernet Speed LED	O-3.3	-	-
A5	GBEO_LINK1000#	GBEO_LINK1000# / Ethernet Speed LED	O-3.3	-	-
A6	GBEO_MDI2-	GBEO_MDI2_N / Ethernet Receive Data -	DP-I	-	-
A7	GBEO_MDI2+	GBEO_MDI2_P / Ethernet Receive Data -	DP-I	-	-
A8	GBEO_LINK#	GBEO_LINK# / LAN Link LED	OD	-	-
A9	GBEO_MDI1-	GBEO_MDI1_N / Ethernet Receive Data -	DP-I	-	-
A10	GBEO_MDI1+	GBEO_MDI1_P / Ethernet Receive Data +	DP-I	-	-
A11	GND	Power Ground	PWR	-	-
A12	GBEO_MDIO-	GBEO_MDIO_N / Ethernet Transmit Data -	DP-O	-	-
A13	GBEO_MDIO+	GBEO_MDIO_P / Ethernet Transmit Data +	DP-O	-	-
A14	GBEO_CTREF	GBEO_CTREF	O-1,8	-	n. c. on module, because not needed
A15	SUS_S3#	PM_SLP_S3_EXT#	O-3.3	PD 10k	-
A16	SATA0_TX+	SATA_TX0_P / SATA 0 Transmit Data +	DP-O	-	-
A17	SATA0_TX-	SATA_TX0_N / SATA 0 Transmit Data -	DP-O	-	-
A18	SUS_S4#	PM_SLP_S4#	O-3.3	-	-
A19	SATA0_RX+	SATA_RX0_P / SATA 0 Receive Data +	DP-I	-	-
A20	SATA0_RX-	SATA_RX0_N / SATA 0 Receive Data -	DP-I	-	-
A21	GND	Power Ground	PWR	-	-
A22	SATA2_TX+	SATA_TX2_P / SATA 2 Transmit Data +	DP-O	-	-
A23	SATA2_TX-	SATA_TX2_N / SATA 2 Transmit Data -	DP-O	-	-
A24	SUS_S5#	PM_SLP_S5#	O-3.3	-	-
A25	SATA2_RX+	SATA_RX2_P / SATA 2 Receive Data +	DP-I	-	-
A26	SATA2_RX-	SATA_RX2_N / SATA 2 Receive Data -	DP-I	-	-
A27	BATLOW#	PM_BATLOW# / Battery Low	I-3.3	PU 10k 3.3V (S5)	-
A28	ATA_ACT#	ATA_LED# / SATA LED	OD-3.3	PU 10k 3.3V (S0)	can pull down 6mA max.
A29	AC/HDA_SYNC	HDA_SYNC / HD Audio Sync	O-3.3	PD 1MEG	-
A30	AC/HDA_RST#	HDA_RST# / HD Audio Reset	O-3.3	-	-
A31	GND	Power Ground	PWR	-	-
A32	AC/HDA_BITCLK	HDA_BITCLK / HD Audio Clock	O-3.3	-	-
A33	AC/HDA_SDOOUT	HDA_SDOOUT / HD Audio Data	O-3.3	-	int. PD 20k in PCH
A34	BIOS_DIS0#	BIOS_DIS0#	I-3.3	PU 10k 3.3V (S5)	-
A35	THRMTRIP#	EXT_THRMTRIP#	O-3.3	PU 10k 3.3V (S0)	-
A36	USB6-	USB6_N / USB Data - Port6	DP-I/O	-	int. PD 15k in PCH / 5V tolerant
A37	USB6+	USB6_P / USB Data + Port6	DP-I/O	-	int. PD 15k in PCH / 5V tolerant
A38	USB_6_7_OC#	USB_67_OC# / USB OverCurrent Port 6/7	I-3.3	PU 10k 3.3V (S5)	-
A39	USB4-	USB4_N / USB Data - Port4	DP-I/O	-	int. PD 15k in PCH / 5V tolerant
A40	USB4+	USB4_P / USB Data + Port4	DP-I/O	-	int. PD 15k in PCH / 5V tolerant
A41	GND	Power Ground	PWR	-	-
A42	USB2-	USB2_N / USB Data - Port2	DP-I/O	-	int. PD 15k in PCH / 5V tolerant
A43	USB2+	USB2_P / USB Data + Port2	DP-I/O	-	int. PD 15k in PCH / 5V tolerant
A44	USB_2_3_OC#	USB_23_OC# / USB OverCurrent Port 2/3	I-3.3	PU 10k 3.3V (S5)	-
A45	USB0-	USB0_N / USB Data - Port0	DP-I/O	-	int. PD 15k in PCH / 5V tolerant
A46	USB0+	USB0_P / USB Data + Port0	DP-I/O	-	int. PD 15k in PCH / 5V tolerant
A47	VCC_RTC	V_BAT	PWR 3V	-	-
A48	EXCD0_PERST#	EXCD0_PERST#/Express card reset	O-3.3	-	-
A49	EXCD0_CPPE#	EXCD0_CPPE# / capable c. request	I-3.3	PU 10k 3.3V (S0)	-
A50	LPC_SERIRQ	LPC_SERIRQ / Serial Interrupt Request	I/O-3.3	PU 8k2 3.3V (S0)	-
A51	GND	Power Ground	PWR	-	-
A52	PCIE_TX5+	PCI Express lane 5 + Transmit	DP-O	-	-
A53	PCIE_TX5-	PCI Express lane 5 - Transmit	DP-O	-	-
A54	GPIO	EXT_GPIO / General Purpose Input 0	I-3.3	PU 10k 3.3V (S0)	-
A55	PCIE_TX4+	PCI Express lane 4 + Transmit	DP-O	-	-
A56	PCIE_TX4-	PCI Express lane 4 - Transmit	DP-O	-	-
A57	GND	Power Ground	PWR	-	-
A58	PCIE_TX3+	PCI Express lane 3 + Transmit	DP-O	-	-
A59	PCIE_TX3-	PCI Express lane 3 - Transmit	DP-O	-	-
A60	GND	Power Ground	PWR	-	-
A61	PCIE_TX2+	PCI Express lane 2 + Transmit	DP-O	-	-
A62	PCIE_TX2-	PCI Express lane 2 - Transmit	DP-O	-	-
A63	GPI1	EXT_GPI1 / General Purpose Input 1	I-3.3	PU 10k 3.3V (S0)	-
A64	PCIE_TX1+	PCI Express lane 1 + Transmit	DP-O	-	-

A65	PCIE_TX1-	PCI Express lane 1 - Transmit	DP-0	-	-
A66	GND	Power Ground	PWR	-	-
A67	GPI2	EXT_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	-	-
A71	LVDS_A0+/eDP_TX2+	LVDS_A_DATA0_P / eDP_TX2_P	DP-0	-	-
A72	LVDS_A0-/eDP_TX2-	LVDS_A_DATA0_N / eDP_TX2_N	DP-0	-	-
A73	LVDS_A1+/eDP_TX1+	LVDS_A_DATA1_P / eDP_TX1_P	DP-0	-	-
A74	LVDS_A1-/eDP_TX1-	LVDS_A_DATA1_N / eDP_TX1_N	DP-0	-	-
A75	LVDS_A2+/eDP_TX0+	LVDS_A_DATA2_P / eDP_TX0_P	DP-0	-	-
A76	LVDS_A2-/eDP_TX0-	LVDS_A_DATA2_N / eDP_TX0_N	DP-0	-	-
A77	LVDS/eDP_VDD_EN	LVDS/eDP_VDD_EN / LVDS/eDP Panel Power Control	0-3.3	PD 100k	-
A78	LVDS_A3+	LVDS_A_DATA3_P / LVDS Channel A Data3+	DP-0	-	-
A79	LVDS_A3-	LVDS_A_DATA3_N / LVDS Channel A Data3-	DP-0	-	-
A80	GND	Power Ground	PWR	-	-
A81	LVDS_A_CLK+/eDP_TX3+	LVDS_A_CLK_P / eDP_TX3_P / LVDS Ch A Clock+	DP-0	-	-
A82	LVDS_A_CLK-/eDP_TX3-	LVDS_A_CLK_N / eDP_TX3_N / LVDS Ch A Clock-	DP-0	-	-
A83	LVDS_I2C_CLK/eDP_AUX+	LVDS_DDC_CLK / eDP_AUX_P / LVDS I2C Clock	I/0-3.3	PU 2k21 3.3V (S0)	-
A84	LVDS_I2C_DAT/eDP_AUX-	LVDS_DDC_DATA / eDP_AUX_N / LVDS I2C Data	I/0-3.3	PU 2k21 3.3V (S0)	-
A85	GPI3	EXT_GPI3 / General Purpose Input 3	I-3.3	PU 10k 3.3V (S0)	strapping function (if pulled low till release of CB_RESET#, LVDS is disabled to enable eDP)
A86	RSVD	n.c.	Nc	-	-
A87	RSVD/eDP_HPD	n.c. / eDP Hot Plug Detect	DP-0	-	-
A88	PCIE_CLK_REF+	CLK_PCIE_REF_P / PCIE Reference Clock	DP-0	-	-
A89	PCIE_CLK_REF-	CLK_PCIE_REF_N / PCIE Reference Clock	DP-0	-	-
A90	GND	Power Ground	PWR	-	-
A91	SPI_POWER	V3.3_SPI_POWER	0-3.3	-	power supply pin for external SPI flash
A92	SPI_MISO	SPI_S0 / SPI slave output	I-3.3	-	int. PU 20k in PCH
A93	GP00	EXT_GP00 / General Purpose Output 0	0-3.3	PD 10k	-
A94	SPI_CLK	SPI_CLK / SPI clock	0-3.3	-	-
A95	SPI_MOSI	SPI_SI / SPI slave input	0-3.3	-	int. PD 20k in PCH
A96	TPM_PP	TPM Physical Presence	I-3.3	PD 100k	-
A97	TYPE10#	n.c. for type 2 module	Nc	-	-
A98	SER0_TX	serial port 0 TXD	0-3.3	-	-
A99	SER0_RX	serial port 0 RXD	I-3.3	PU 47K 3.3V (S0)	-
A100	GND	Power Ground	PWR	-	-
A101	SER1_TX	serial port 1 TXD	0-3.3	-	-
A102	SER1_RX	serial port 1 RXD	I-3.3	PU 47K 3.3V (S0)	-
A103	LID#	LID switch input	I-3.3	PU 10K 3.3V (S5)	-
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	-	-

7.3 Connector X1A Row B

Pin	Signal	Description	Type	Termination	Comment
B1	GND	Power Ground	PWR	-	-
B2	GBE0_ACT#	GBE0_ACT# / Ethernet Activity LED	OD	-	-
B3	LPC_FRAME#	LPC_FRAME# / LPC Frame Indicator	0-3.3	-	-
B4	LPC_AD0	LPC_AD0 / LPC Address & DATA Bus	I/O-3.3	-	int. PU 20k in PCH
B5	LPC_AD1	LPC_AD1 / LPC Address & DATA Bus	I/O-3.3	-	int. PU 20k in PCH
B6	LPC_AD2	LPC_AD2 / LPC Address & DATA Bus	I/O-3.3	-	int. PU 20k in PCH
B7	LPC_AD3	LPC_AD3 / LPC Address & DATA Bus	I/O-3.3	-	int. PU 20k in PCH
B8	LPC_DRQ0#	LPC_DRQ0# / LPC Request 0	I-3.3	PU 2k 3.3V (S0)	int. PU 20k in PCH
B9	LPC_DRQ1#	LPC_DRQ1# / LPC Request 1	I-3.3	PU 2k 3.3V (S0)	int. PU 20k in PCH
B10	LPC_CLK	CLK_LPC_33M_EXT / 33MHz LPC clock	0-3.3	-	-
B11	GND	Power Ground	PWR	-	-
B12	PWRBTN#	EXT_PWRBTN# / Power Button	I-3.3	PU 10k 3.3V (S5eco)	-
B13	SMB_CLK	SMB_CLK_EXT / SMBUS Clock	0-3.3	PU 3k3 3.3V (S5)	-
B14	SMB_DAT	SMB_DATA_EXT / SMBUS Data	I/O-3.3	PU 3k3 3.3V (S5)	-
B15	SMB_ALERT#	SMB_ALERT# / SMBUS Interrupt	I/O-3.3	PU 1k0 3.3V (S5)	-
B16	SATA1_TX+	SATA_TX1_P / SATA 1 Transmit Data +	DP-0	-	-
B17	SATA1_TX-	SATA_TX1_N / SATA 1 Transmit Data -	DP-0	-	-
B18	SUS_STAT#	PM_SUS_STAT#	0-3.3	-	-
B19	SATA1_RX+	SATA_RX1_P / SATA 1 Receive Data +	DP-I	-	-
B20	SATA1_RX-	SATA_RX1_N / SATA 1 Receive Data -	DP-I	-	-
B21	GND	Power Ground	PWR	-	-
B22	SATA3_TX+	SATA_TX3_P / SATA 3 Transmit Data +	DP-0	-	-
B23	SATA3_TX-	SATA_TX3_N / SATA 3 Transmit Data -	DP-0	-	-
B24	PWR_OK	EXT_PWR_OK / Power OK	I-3.3	PU 511k 3.3V (S5)	pullup voltage depends on ATX or single supply mode / 5V tolerant
B25	SATA3_RX+	SATA_RX3_P / SATA 3 Receive Data +	DP-I	-	-
B26	SATA3_RX-	SATA_RX3_N / SATA 3 Receive Data -	DP-I	-	-
B27	WDT	WDT / Watch Dog Timer	0-3.3	-	-
B28	AC/HDA_SDIN2	HDA_SDIN2_ICH/ HD Audio Serial Input Data 2	I-3.3	-	int. PD 20k in PCH
B29	AC/HDA_SDIN1	HDA_SDIN1_ICH/ HD Audio Serial Input Data 1	I-3.3	-	int. PD 20k in PCH
B30	AC/HDA_SDINO	HDA_SDINO_ICH/ HD Audio Serial Input Data 0	I-3.3	-	int. PD 20k in PCH
B31	GND	Power Ground	PWR	-	-
B32	SPKR	HDA_SPKR / Speaker	0-3.3	-	int. PD 20k in PCH
B33	I2C_CLK	I2C_CLK_EXT / I2C clock	0-3.3	PU 2k21 3.3V (S5)	-
B34	I2C_DAT	I2C_DATA_EXT / I2C data	I/O-3.3	PU 2k21 3.3V (S5)	-
B35	THRM#	PM_THRM# / Over Temperature	I-3.3	PU 10k 3.3V (S0)	-
B36	USB7-	USB7_N / USB Data - Port7	DP-I/O	-	int. PD 15k in PCH / 5V tolerant
B37	USB7+	USB7_P / USB Data + Port7	DP-I/O	-	int. PD 15k in PCH / 5V tolerant
B38	USB_4_5_OC#	USB_45_OC# / USB OverCurrent Port 4/5	I-3.3	PU 10k 3.3V (S5)	-
B39	USB5-	USB5_N / USB Data - Port5	DP-I/O	-	int. PD 15k in PCH / 5V tolerant
B40	USB5+	USB5_P / USB Data + Port5	DP-I/O	-	int. PD 15k in PCH / 5V tolerant
B41	GND	Power Ground	PWR	-	-
B42	USB3-	USB3_N / USB Data - Port3	DP-I/O	-	int. PD 15k in PCH / 5V tolerant
B43	USB3+	USB3_P / USB Data + Port3	DP-I/O	-	int. PD 15k in PCH / 5V tolerant
B44	USB_0_1_OC#	USB_01_OC# / USB OverCurrent Port 0/1	I-3.3	PU 10k 3.3V (S5)	-
B45	USB1-	USB1_N / USB Data - Port1	DP-I/O	-	int. PD 15k in PCH / 5V tolerant
B46	USB1+	USB1_P / USB Data + Port1	DP-I/O	-	int. PD 15k in PCH / 5V tolerant
B47	EXCD1_PERST#	EXCD1_PERST# / Express card reset	0-3.3	-	-
B48	EXCD1_CPPE#	EXCD1_CPPE# / capable c. request	I-3.3	PU 10k 3.3V (S0)	-
B49	SYS_RESET#	EXT_SYS_RESET# / Reset Input	I-3.3	PU 10k 3.3V (S5)	-
B50	CB_RESET#	CB_RESET# / Carrier board Reset	0-3.3	PU 10k 3.3V (S5)	-
B51	GND	Power Ground	PWR	-	-
B52	PCIE_RX5+	PCI Express lane 5 + receive	DP-I	-	-
B53	PCIE_RX5-	PCI Express lane 5 - receive	DP-I	-	-
B54	GP01	EXT_GP01 / 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	GP02	EXT_GP02 / 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	-	-
B61	PCIE_RX2+	PCI Express lane 2 + receive	DP-I	-	-
B62	PCIE_RX2-	PCI Express lane 2 - receive	DP-I	-	-
B63	GP03	EXT_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#	PCIE_WAKE#	I/O-3.3	PU 1k2 3.3V (S5)	-
B67	WAKE1#	WAKE1#	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	-	-
B71	LVDS_B0+	LVDS_B_DATA0_P / LVDS Channel B Data0+	DP-0	-	-
B72	LVDS_B0-	LVDS_B_DATA0_N / LVDS Channel B Data0-	DP-0	-	-
B73	LVDS_B1+	LVDS_B_DATA1_P / LVDS Channel B Data1+	DP-0	-	-
B74	LVDS_B1-	LVDS_B_DATA1_N / LVDS Channel B Data1-	DP-0	-	-
B75	LVDS_B2+	LVDS_B_DATA2_P / LVDS Channel B Data2+	DP-0	-	-
B76	LVDS_B2-	LVDS_B_DATA2_N / LVDS Channel B Data2 -	DP-0	-	-
B77	LVDS_B3+	LVDS_B_DATA3_P / LVDS Channel B Data3+	DP-0	-	-
B78	LVDS_B3-	LVDS_B_DATA3_N / LVDS Channel B Data3-	DP-0	-	-
B79	LVDS/eDP_BKLT_EN	LVDS_eDP_BKLT_EN / Panel Backlight ON	0-3.3	PD 100k	-
B80	GND	Power Ground	PWR	-	-
B81	LVDS_B_CLK+	LVDS_B_CLK_P / LVDS Channel B Clock+	DP-0	-	-
B82	LVDS_B_CLK-	LVDS_B_CLK_N / LVDS Channel B Clock-	DP-0	-	-
B83	LVDS/eDP_BKLT_CTRL	LVDS_eDP_BKLT_CTRL / Backlight Brightness Contr.	0-3.3	-	-
B84	VCC_5V_SBY	+V_STBY_ETX / 5V Standby	PWR 5V (S5)	-	optional (not necessary in single supply mode)
B85	VCC_5V_SBY	+V_STBY_ETX / 5V Standby	PWR 5V (S5)	-	optional (not necessary in single supply mode)
B86	VCC_5V_SBY	+V_STBY_ETX / 5V Standby	PWR 5V (S5)	-	optional (not necessary in single supply mode)
B87	VCC_5V_SBY	+V_STBY_ETX / 5V Standby	PWR 5V (S5)	-	optional (not necessary in single supply mode)
B88	BIOS_DIS1#	BIOS_DIS1#	I-3.3	PU 10k 3.3V (S5)	-
B89	VGA_RED	CRT_RED / Analog Video RGB-RED	OA	PD 150R	not available on Haswell ULT
B90	GND	Power Ground	PWR	-	-
B91	VGA_GRN	CRT_GREEN / Analog Video RGB-GREEN	OA	PD 150R	not available on Haswell ULT
B92	VGA_BLU	CRT_BLUE / Analog Video RGB-BLUE	OA	PD 150R	not available on Haswell ULT
B93	VGA_HSYNC	CRT_HSYNC / Analog Video H-Sync	0-3.3	-	not available on Haswell ULT
B94	VGA_VSYNC	CRT_VSYNC / Analog Video V-Sync	0-3.3	-	not available on Haswell ULT
B95	VGA_I2C_CLK	CRT_DDC_CLK / Display Data Channel Clock	I/O-3.3	PU 1k1 3.3V (S0)	not available on Haswell ULT
B96	VGA_I2C_DAT	CRT_DDC_DATA / Display Data Channel Data	I/O-3.3	PU 1k1 3.3V (S0)	not available on Haswell ULT
B97	SPI_CS#	SPI_CS# / SPI chip select	0-3.3	-	-
B98	RSVD	n. c.	nc	-	-
B99	RSVD	n. c.	nc	-	-
B100	GND	Power Ground	PWR	-	-
B101	FAN_PWMOUT	Fan PWM Output	0-3.3	-	-
B102	FAN_TACHIN	Fan Tach Input	I-3.3	PU 10K 3.3V (S0)	-
B103	SLEEP#	Sleep Button Input	I-3.3	PU 10K 3.3V (S5)	-
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	-	-

7.4 Connector X1B Row C

Pin	Signal	Description	Type	Termination	Comment
C1	GND	Power Ground	PWR	-	-
C2	GND	Power Ground	PWR	-	-
C3	USB_SSRX0-	USB Super Speed Receive - (0)	DP-I	-	-
C4	USB_SSRX0+	USB Super Speed Receive + (0)	DP-I	-	-
C5	GND	Power Ground	PWR	-	-
C6	USB_SSRX1-	USB Super Speed Receive - (1)	DP-I	-	-
C7	USB_SSRX1+	USB Super Speed Receive + (1)	DP-I	-	-
C8	GND	Power Ground	PWR	-	-
C9	USB_SSRX2-	USB Super Speed Receive - (2)	DP-I	-	not available on cHL6 module
C10	USB_SSRX2+	USB Super Speed Receive + (2)	DP-I	-	not available on cHL6 module
C11	GND	Power Ground	PWR	-	-
C12	USB_SSRX3-	USB Super Speed Receive - (3)	DP-I	-	not available on cHL6 module
C13	USB_SSRX3+	USB Super Speed Receive + (3)	DP-I	-	not available on cHL6 module
C14	GND	Power Ground	PWR	-	-
C15	DDI1_PAIR6+	DDI1 Pair 6 +	DP-I	-	not available on cHL6 module
C16	DDI1_PAIR6-	DDI1 Pair 6 -	DP-I	-	not available on cHL6 module
C17	RSVD	n.c.	Nc	-	-
C18	RSVD	n.c.	Nc	-	-
C19	PCIE_RX6+	PCI Express lane 6 + receive	DP-I	-	not available on cHL6 module
C20	PCIE_RX6-	PCI Express lane 6 - receive	DP-I	-	not available on cHL6 module
C21	GND	Power Ground	PWR	-	-
C22	PCIE_RX7+	opt. PCI Express lane 7 + Receive	DP-I	-	-
C23	PCIE_RX7-	opt. PCI Express lane 7 - Receive	DP-I	-	-
C24	DDI1_HPD	DDI1 Hotplug Detect	I-3.3	PD 100k	-
C25	DDI1_PAIR4+	DDI1 Pair 4 +	DP-I	-	not available on cHL6 module
C26	DDI1_PAIR4-	DDI1 Pair 4 -	DP-I	-	not available on cHL6 module
C27	RSVD	n.c.	Nc	-	-
C28	RSVD	n.c.	Nc	-	-
C29	DDI1_PAIR5+	DDI1 Pair 5 +	DP-I	-	not available on cHL6 module
C30	DDI1_PAIR5-	DDI1 Pair 5 -	DP-I	-	not available on cHL6 module
C31	GND	Power Ground	PWR	-	-
C32	DDI2_CTRLCLK_AUX+	DDI2 CTRLCLK/AUX+	I/O-3.3	PD 100k	-
C33	DDI2_CTRLCLK_AUX-	DDI2 CTRLCLK/AUX-	I/O-3.3	PU 100k 3.3 (S0)	-
C34	DDI2_DDC_AUX_SEL	DDI2 DDC/AUX select	I-3.3	PD 1M	-
C35	RSVD	n.c.	Nc	-	-
C36	DDI3_CTRLCLK_AUX+	DDI3 CTRLCLK/AUX+	I/O-3.3	-	not available on cHL6 module
C37	DDI3_CTRLCLK_AUX-	DDI3 CTRLCLK/AUX-	I/O-3.3	-	not available on cHL6 module
C38	DDI3_DDC_AUX_SEL	DDI3 DDC/AUX select	I-3.3	-	not available on cHL6 module
C39	DDI3_PAIR0+	DDI3 Pair 0 +	DP-0	-	not available on cHL6 module
C40	DDI3_PAIR0-	DDI3 Pair 0 -	DP-0	-	not available on cHL6 module
C41	GND	Power Ground	PWR	-	-
C42	DDI3_PAIR1+	DDI3 Pair 1 +	DP-0	-	not available on cHL6 module
C43	DDI3_PAIR1-	DDI3 Pair 1 -	DP-0	-	not available on cHL6 module
C44	DDI3_HPD	DDI3 Hotplug Detect	I-3.3	-	not available on cHL6 module
C45	RSVD	n.c.	Nc	-	-
C46	DDI3_PAIR2+	DDI3 Pair 2 +	DP-0	-	not available on cHL6 module
C47	DDI3_PAIR2-	DDI3 Pair 2 -	DP-0	-	not available on cHL6 module
C48	RSVD	n.c.	Nc	-	-
C49	DDI3_PAIR3+	DDI3 Pair 3 +	DP-0	-	not available on cHL6 module
C50	DDI3_PAIR3-	DDI3 Pair 3 -	DP-0	-	not available on cHL6 module
C51	GND	Power Ground	PWR	-	-
C52	PEG_RX0+	PCIexpress Graphics receive + (0)	DP-I	-	not available on cHL6 module
C53	PEG_RX0-	PCIexpress Graphics receive - (0)	DP-I	-	not available on cHL6 module
C54	TYPE0#	n.c. for type 6 module	nc	-	-
C55	PEG_RX1+	PCIexpress Graphics receive + (1)	DP-I	-	not available on cHL6 module
C56	PEG_RX1-	PCIexpress Graphics receive - (1)	DP-I	-	not available on cHL6 module
C57	TYPE1#	n.c. for type 6 module	nc	-	-
C58	PEG_RX2+	PCIexpress Graphics receive + (2)	DP-I	-	not available on cHL6 module
C59	PEG_RX2-	PCIexpress Graphics receive - (2)	DP-I	-	not available on cHL6 module
C60	GND	Power Ground	PWR	-	-
C61	PEG_RX3+	PCIexpress Graphics receive + (3)	DP-I	-	not available on cHL6 module
C62	PEG_RX3-	PCIexpress Graphics receive - (3)	DP-I	-	not available on cHL6 module
C63	RSVD	n.c.	nc	-	-
C64	RSVD	n.c.	nc	-	-

C65	PEG_RX4+	PCIexpress Graphics receive + (4)	DP-I	-	not available on cHL6 module
C66	PEG_RX4-	PCIexpress Graphics receive - (4)	DP-I	-	not available on cHL6 module
C67	RSVD	n.c.	nc	-	-
C68	PEG_RX5+	PCIexpress Graphics receive + (5)	DP-I	-	not available on cHL6 module
C69	PEG_RX5-	PCIexpress Graphics receive - (5)	DP-I	-	not available on cHL6 module
C70	GND	Power Ground	PWR	-	-
C71	PEG_RX6+	PCIexpress Graphics receive + (6)	DP-I	-	not available on cHL6 module
C72	PEG_RX6-	PCIexpress Graphics receive - (6)	DP-I	-	not available on cHL6 module
C73	GND	Power Ground	PWR	-	-
C74	PEG_RX7+	PCIexpress Graphics receive + (7)	DP-I	-	not available on cHL6 module
C75	PEG_RX7-	PCIexpress Graphics receive - (7)	DP-I	-	not available on cHL6 module
C76	GND	Power Ground	PWR	-	-
C77	RSVD	n.c.	nc	-	-
C78	PEG_RX8+	PCIexpress Graphics receive + (8)	DP-I	-	not available on cHL6 module
C79	PEG_RX8-	PCIexpress Graphics receive - (8)	DP-I	-	not available on cHL6 module
C80	GND	Power Ground	PWR	-	-
C81	PEG_RX9+	PCIexpress Graphics receive + (9)	DP-I	-	not available on cHL6 module
C82	PEG_RX9-	PCIexpress Graphics receive - (9)	DP-I	-	not available on cHL6 module
C83	RSVD	n.c.	nc	-	-
C84	GND	Power Ground	PWR	-	-
C85	PEG_RX10+	PCIexpress Graphics receive + (10)	DP-I	-	not available on cHL6 module
C86	PEG_RX10-	PCIexpress Graphics receive - (10)	DP-I	-	not available on cHL6 module
C87	GND	Power Ground	PWR	-	-
C88	PEG_RX11+	PCIexpress Graphics receive + (11)	DP-I	-	not available on cHL6 module
C89	PEG_RX11-	PCIexpress Graphics receive - (11)	DP-I	-	not available on cHL6 module
C90	GND	Power Ground	PWR	-	-
C91	PEG_RX12+	PCIexpress Graphics receive + (12)	DP-I	-	not available on cHL6 module
C92	PEG_RX12-	PCIexpress Graphics receive - (12)	DP-I	-	not available on cHL6 module
C93	GND	Power Ground	PWR	-	-
C94	PEG_RX13+	PCIexpress Graphics receive + (13)	DP-I	-	not available on cHL6 module
C95	PEG_RX13-	PCIexpress Graphics receive - (13)	DP-I	-	not available on cHL6 module
C96	GND	Power Ground	PWR	-	-
C97	RSVD	n.c.	nc	-	-
C98	PEG_RX14+	PCIexpress Graphics receive + (14)	DP-I	-	not available on cHL6 module
C99	PEG_RX14-	PCIexpress Graphics receive - (14)	DP-I	-	not available on cHL6 module
C100	GND	Power Ground	PWR	-	-
C101	PEG_RX15+	PCIexpress Graphics receive + (15)	DP-I	-	not available on cHL6 module
C102	PEG_RX15-	PCIexpress Graphics receive - (15)	DP-I	-	not available on cHL6 module
C103	GND	Power Ground	PWR	-	-
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	-	-

7.5 Connector X1B Row D

Pin	Signal	Description	Type	Termination	Comment
D1	GND	Power Ground	PWR	-	-
D2	GND	Power Ground	PWR	-	-
D3	USB_SSTX0-	USB Super Speed Transmit - (0)	DP-0	-	-
D4	USB_SSTX0+	USB Super Speed Transmit + (0)	DP-0	-	-
D5	GND	Power Ground	PWR	-	-
D6	USB_SSTX1-	USB Super Speed Transmit - (1)	DP-0	-	-
D7	USB_SSTX1+	USB Super Speed Transmit + (1)	DP-0	-	-
D8	GND	Power Ground	PWR	-	-
D9	USB_SSTX2-	USB Super Speed Transmit - (2)	DP-0	-	not available on cHL6 module
D10	USB_SSTX2+	USB Super Speed Transmit + (2)	DP-0	-	not available on cHL6 module
D11	GND	Power Ground	PWR	-	-
D12	USB_SSTX3-	USB Super Speed Transmit - (3)	DP-0	-	not available on cHL6 module
D13	USB_SSTX3+	USB Super Speed Transmit + (3)	DP-0	-	not available on cHL6 module
D14	GND	Power Ground	PWR	-	-
D15	DDI1_CTRLCLK_AUX+	DDI1 CTRLCLK/AUX+	I/O-3.3	PD 100k	-
D16	DDI1_CTRLCLK_AUX-	DDI1 CTRLCLK/AUX-	I/O-3.3	PU 100k 3.3 (S0)	-
D17	RSVD	n.c.	Nc	-	-
D18	RSVD	n.c.	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	-	-
D22	PCIE_TX7+	opt. PCI Express lane 7 + Transmit	DP-0	-	-
D23	PCIE_TX7-	opt. PCI Express lane 7 - Transmit	DP-0	-	-
D24	RSVD	n.c.	Nc	-	-
D25	RSVD	n.c.	Nc	-	-
D26	DDI1_PAIR0+	DDI1 Pair 0 +	DP-0	-	-
D27	DDI1_PAIR0-	DDI1 Pair 0 -	DP-0	-	-
D28	RSVD	n.c.	Nc	-	-
D29	DDI1_PAIR1+	DDI1 Pair 1 +	DP-0	-	-
D30	DDI1_PAIR1-	DDI1 Pair 1 -	DP-0	-	-
D31	GND	Power Ground	PWR	-	-
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	n.c.	Nc	-	-
D36	DDI1_PAIR3+	DDI1 Pair 3 +	DP-0	-	-
D37	DDI1_PAIR3-	DDI1 Pair 3 -	DP-0	-	-
D38	RSVD	n.c.	Nc	-	-
D39	DDI2_PAIR0+	DDI2 Pair 0 +	DP-0	-	-
D40	DDI2_PAIR0-	DDI2 Pair 0 -	DP-0	-	-
D41	GND	Power Ground	PWR	-	-
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	n.c.	Nc	-	-
D46	DDI2_PAIR2+	DDI2 Pair 2 +	DP-0	-	-
D47	DDI2_PAIR2-	DDI2 Pair 2 -	DP-0	-	-
D48	RSVD	n.c.	Nc	-	-
D49	DDI2_PAIR3+	DDI2 Pair 3 +	DP-0	-	-
D50	DDI2_PAIR3-	DDI2 Pair 3 -	DP-0	-	-
D51	GND	Power Ground	PWR	-	-
D52	PEG_TX0+	PCIexpress Graphics Transmit + (0)	DP-0	-	not available on cHL6 module
D53	PEG_TX0-	PCIexpress Graphics Transmit - (0)	DP-0	-	not available on cHL6 module
D54	PEG_LANE_RV#	PCIexpress Graphics Lane Reversal	I-3.3	-	not available on cHL6 module
D55	PEG_TX1+	PCIexpress Graphics Transmit + (1)	DP-0	-	not available on cHL6 module
D56	PEG_TX1-	PCIexpress Graphics Transmit - (1)	DP-0	-	not available on cHL6 module
D57	TYPE2#	GND for type 6 module	O-PWR	-	-
D58	PEG_TX2+	PCIexpress Graphics Transmit + (2)	DP-0	-	not available on cHL6 module
D59	PEG_TX2-	PCIexpress Graphics Transmit - (2)	DP-0	-	not available on cHL6 module
D60	GND	Power Ground	PWR	-	-
D61	PEG_TX3+	PCIexpress Graphics Transmit + (3)	DP-0	-	not available on cHL6 module
D62	PEG_TX3-	PCIexpress Graphics Transmit - (3)	DP-0	-	not available on cHL6 module
D63	RSVD	n.c.	Nc	-	-
D64	RSVD	n.c.	Nc	-	-

D65	PEG_TX4+	PCIexpress Graphics Transmit + (4)	DP-0	-	not available on cHL6 module
D66	PEG_TX4-	PCIexpress Graphics Transmit - (4)	DP-0	-	not available on cHL6 module
D67	GND	Power Ground	PWR	-	-
D68	PEG_TX5+	PCIexpress Graphics Transmit + (5)	DP-0	-	not available on cHL6 module
D69	PEG_TX5-	PCIexpress Graphics Transmit - (5)	DP-0	-	not available on cHL6 module
D70	GND	Power Ground	PWR	-	-
D71	PEG_TX6+	PCIexpress Graphics Transmit + (6)	DP-0	-	not available on cHL6 module
D72	PEG_TX6-	PCIexpress Graphics Transmit - (6)	DP-0	-	not available on cHL6 module
D73	GND	Power Ground	PWR	-	-
D74	PEG_TX7+	PCIexpress Graphics Transmit + (7)	DP-0	-	not available on cHL6 module
D75	PEG_TX7-	PCIexpress Graphics Transmit - (7)	DP-0	-	not available on cHL6 module
D76	GND	Power Ground	PWR	-	-
D77	RSVD	n.c.	Nc	-	-
D78	PEG_TX8+	PCIexpress Graphics Transmit + (8)	DP-0	-	not available on cHL6 module
D79	PEG_TX8-	PCIexpress Graphics Transmit - (8)	DP-0	-	not available on cHL6 module
D80	GND	Power Ground	PWR	-	-
D81	PEG_TX9+	PCIexpress Graphics Transmit + (9)	DP-0	-	not available on cHL6 module
D82	PEG_TX9-	PCIexpress Graphics Transmit - (9)	DP-0	-	not available on cHL6 module
D83	RSVD	n.c.	Nc	-	-
D84	GND	Power Ground	PWR	-	-
D85	PEG_TX10+	PCIexpress Graphics Transmit + (10)	DP-0	-	not available on cHL6 module
D86	PEG_TX10-	PCIexpress Graphics Transmit - (10)	DP-0	-	not available on cHL6 module
D87	GND	Power Ground	PWR	-	-
D88	PEG_TX11+	PCIexpress Graphics Transmit + (11)	DP-0	-	not available on cHL6 module
D89	PEG_TX11-	PCIexpress Graphics Transmit - (11)	DP-0	-	not available on cHL6 module
D90	GND	Power Ground	PWR	-	-
D91	PEG_TX12+	PCIexpress Graphics Transmit + (12)	DP-0	-	not available on cHL6 module
D92	PEG_TX12-	PCIexpress Graphics Transmit - (12)	DP-0	-	not available on cHL6 module
D93	GND	Power Ground	PWR	-	-
D94	PEG_TX13+	PCIexpress Graphics Transmit + (13)	DP-0	-	not available on cHL6 module
D95	PEG_TX13-	PCIexpress Graphics Transmit - (13)	DP-0	-	not available on cHL6 module
D96	GND	Power Ground	PWR	-	-
D97	RSVD	n.c.	Nc	-	-
D98	PEG_TX14+	PCIexpress Graphics Transmit + (14)	DP-0	-	not available on cHL6 module
D99	PEG_TX14-	PCIexpress Graphics Transmit - (14)	DP-0	-	not available on cHL6 module
D100	GND	Power Ground	PWR	-	-
D101	PEG_TX15+	PCIexpress Graphics Transmit + (15)	DP-0	-	not available on cHL6 module
D102	PEG_TX15-	PCIexpress Graphics Transmit - (15)	DP-0	-	not available on cHL6 module
D103	GND	Power Ground	PWR	-	-
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	-	-



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 (depending on console Settings F2 may not be supported)

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

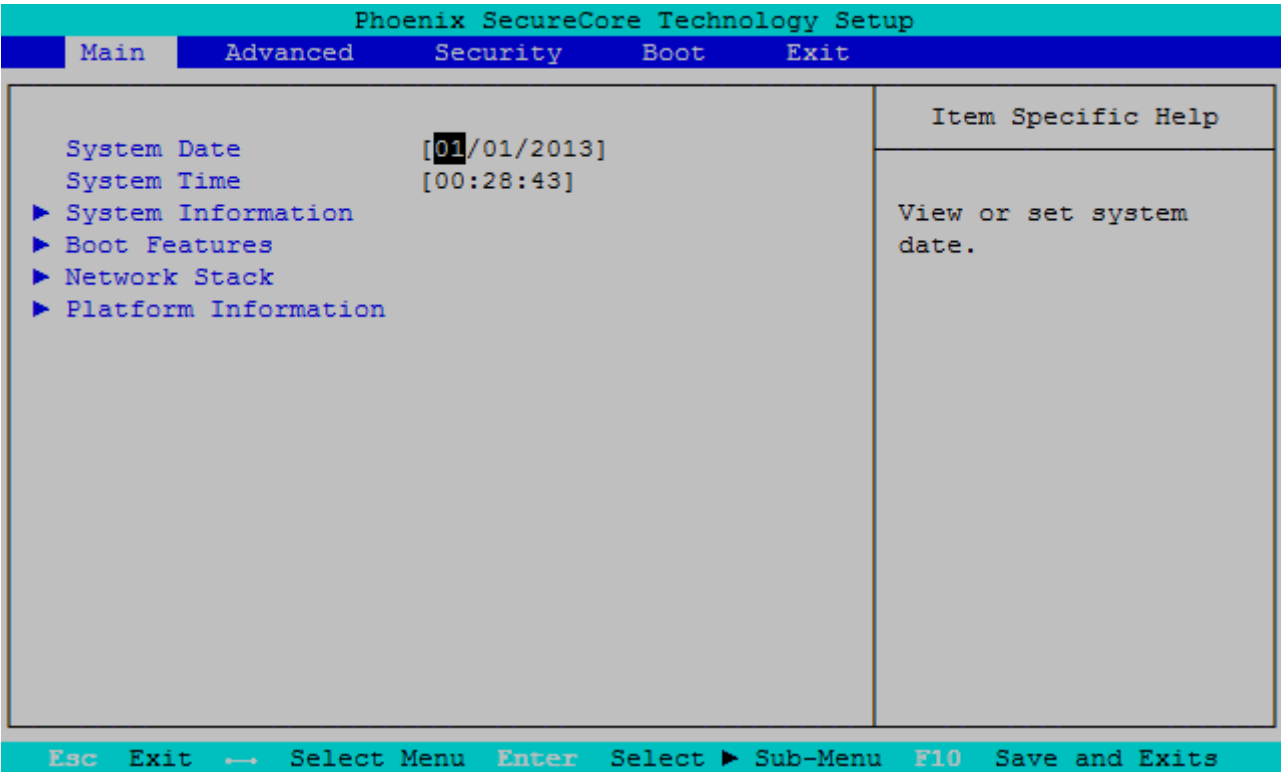
The Help window on the right side of each menu displays the Help text for the selected item. It updates as you move the cursor to each field.

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.

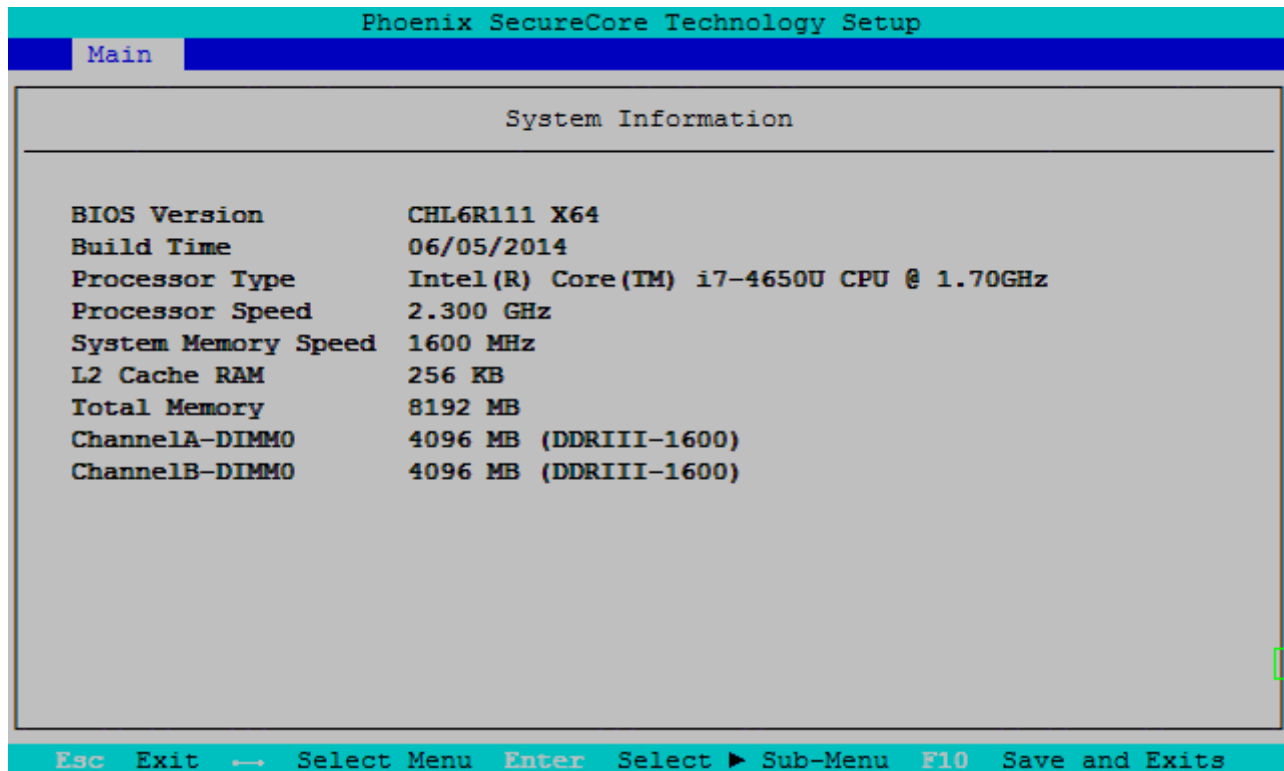
8.5 BIOS Setup

8.5.1 Main

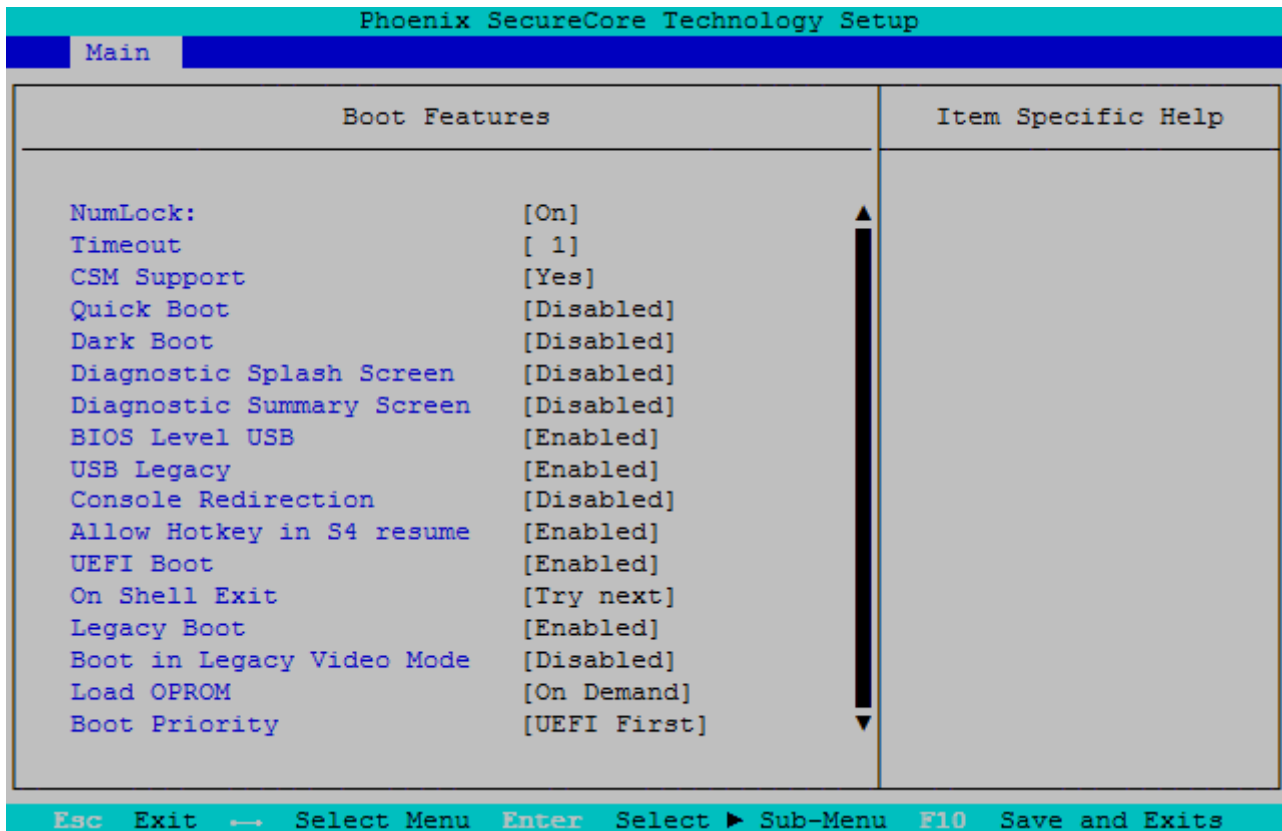


Feature	Options	Description
System Date	[mm/dd/yyyy]	Set the Date. Use 'Tab' to switch between Date elements
System Time	[hh:mm:ss]	Set the Time. Use 'Tab' to switch between Time elements

System Information



Boot Features



Feature	Options	Description
NumLock	On Off	Selects Power-on state for NumLock
Timeout	1	Number of seconds that P.O.S.T will wait for the user input before booting
CSM Support	Yes 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	Disabled Enabled	Enable or Disable Quick Boot
Dark Boot	Disabled Enabled	Enable or Disable Dark Boot
Diagnostic Splash Screen	Disabled Enabled	Enable or Disable the Diagnostic Splash Screen
Diagnostic Summary Screen	Disabled Enabled	Display the Diagnostic Summary Screen during boot
BIOS Level USB	Enabled 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	Enabled Disabled	Enable/Disable USB BIOS SMM support for mouse, keyboard, mass storage, etc, in legacy operating systems such as DOS
Console Redirection	Disabled Enabled	Enable/Disable Universal Console Redirection
- Console Port	All Onboard COM1 Onboard COM2 SIO COM1 SIO COM2	Select Port for console redirection. Note: the respective port has to be enabled in setup!
- Terminal Type	ANSI VT100 VT100+ UTF8	Set terminal type of UCR
- Baudrate	9600 19200 38400 57600 115200	Set terminal type of UCR
- Flow Control	None	Set flow control method for UCR. None = No flow

	RTS/CTS XON/XOFF	control, RTS/CTS = Hardware flow control, XON/XOFF = Software flow control
- Continue C.R. after POST	Enabled Disabled	Enables Console Redirection after OS has loaded
Allow Hotkey in S4 resume	Enabled Disabled	Enable hotkey detection when system resuming from Hybernate state
UEFI Boot	Enabled Disabled	Enable the UEFI boot
On Shell Exit	Try next Launch Setup\Launch Boot Menu	Select behavior after exit from shell
Legacy Boot	Enabled \Disabled	Enable the Legacy boot
Boot in Legacy Video Mode	Disabled 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 OPRM	On Demand All	Load all OPRMs or on demand according to the boot device
Boot Priority	UEFI First 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 Disabled	Enable / Disable UEFI Network Stack
IPv4	Enabled Disabled	Enable / Disable IPv4
UEFI PXE Boot Priority	IPv4 first	Select PXE Boot Priority (IPv4 only)

Platform Information

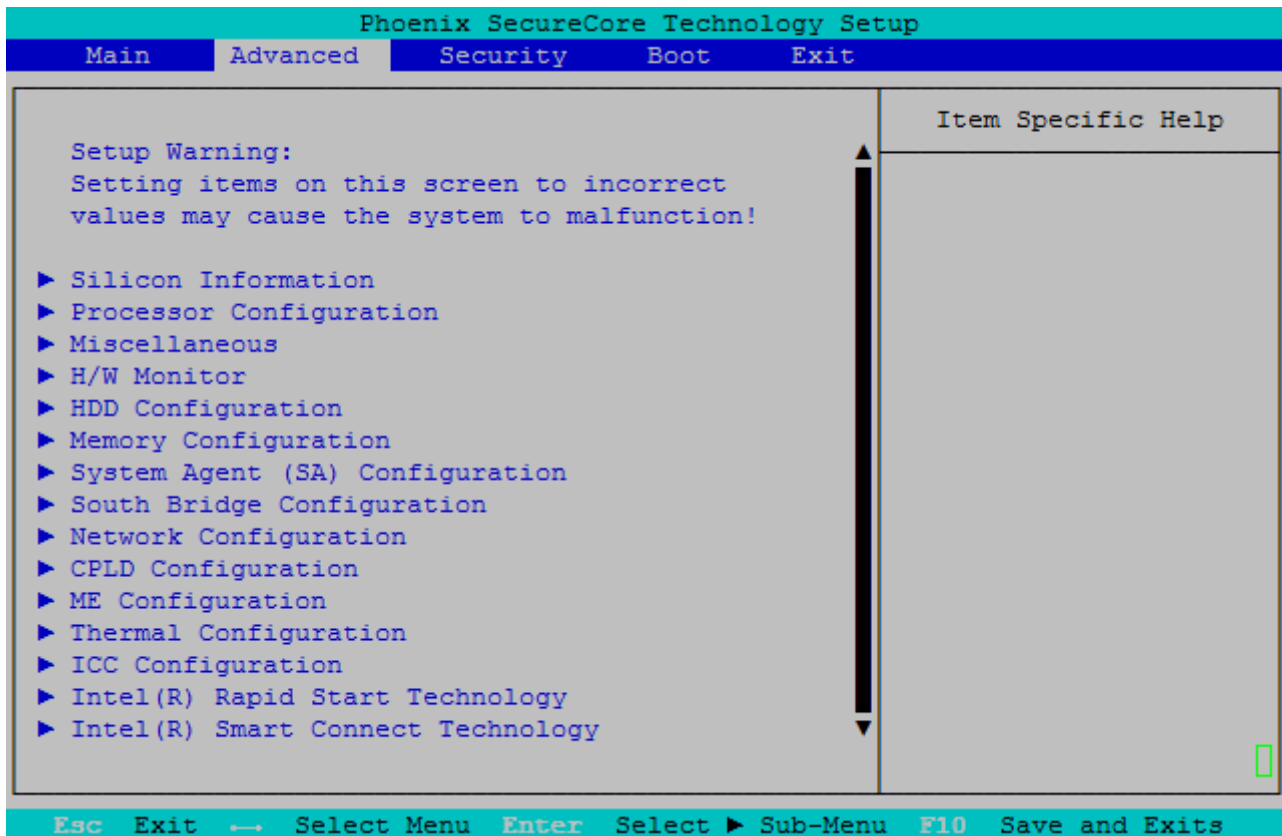
Phoenix SecureCore Technology Setup

Main

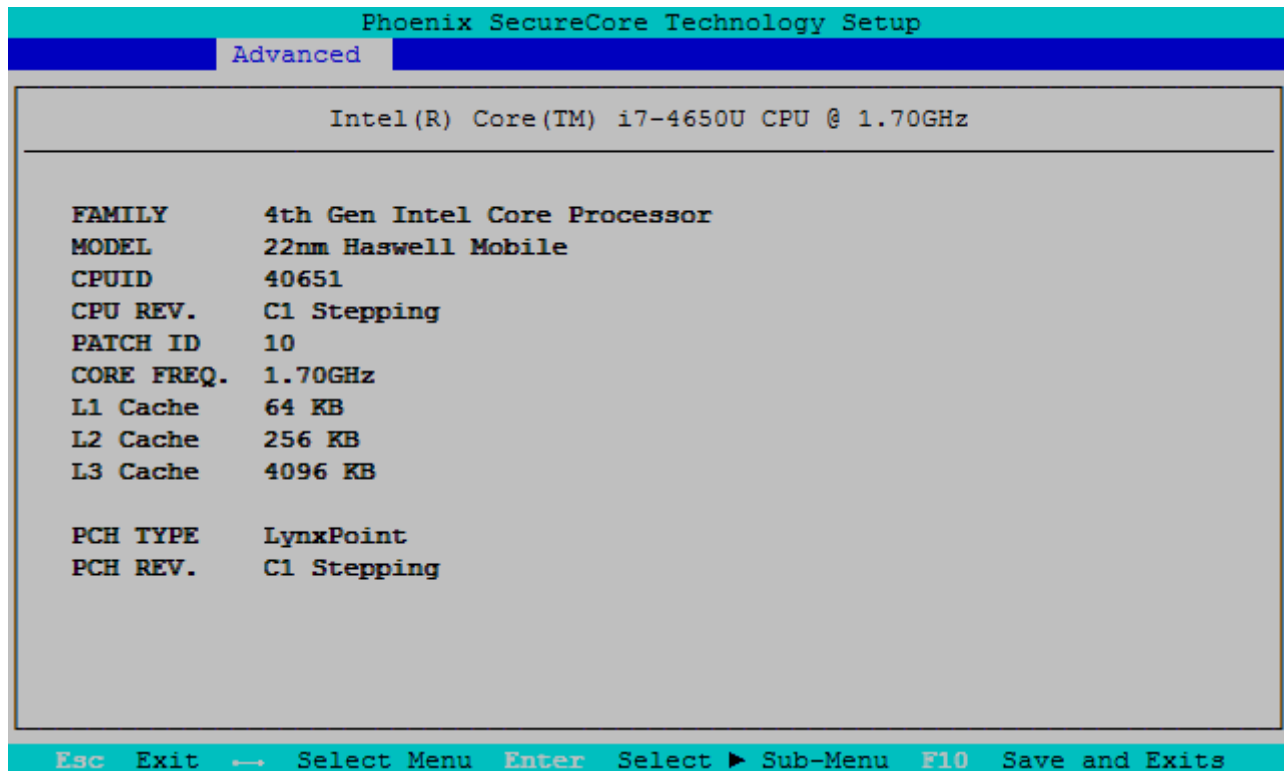
Platform Information	Item Specific Help
Module Information Product NameCOMe-cHL6 Revision1.0.4 Serial #IVD0T0017 MAC Address00:E0:4B:4C:C6:8F CPLD RevP102.001 (Release) Boot Counter8	Platform Information

EscExit↔Select MenuEnterSelect▶Sub-MenuF10Save and Exits

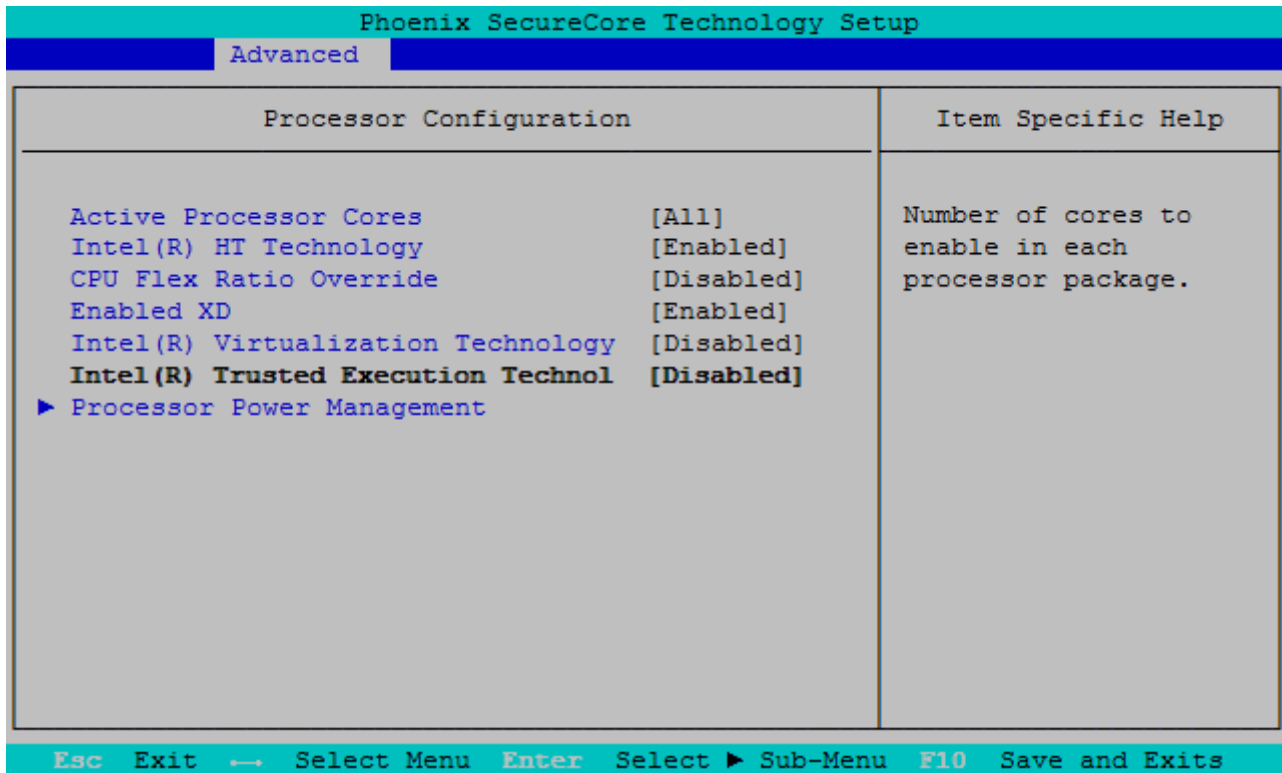
8.5.2 Advanced



Silicon Information

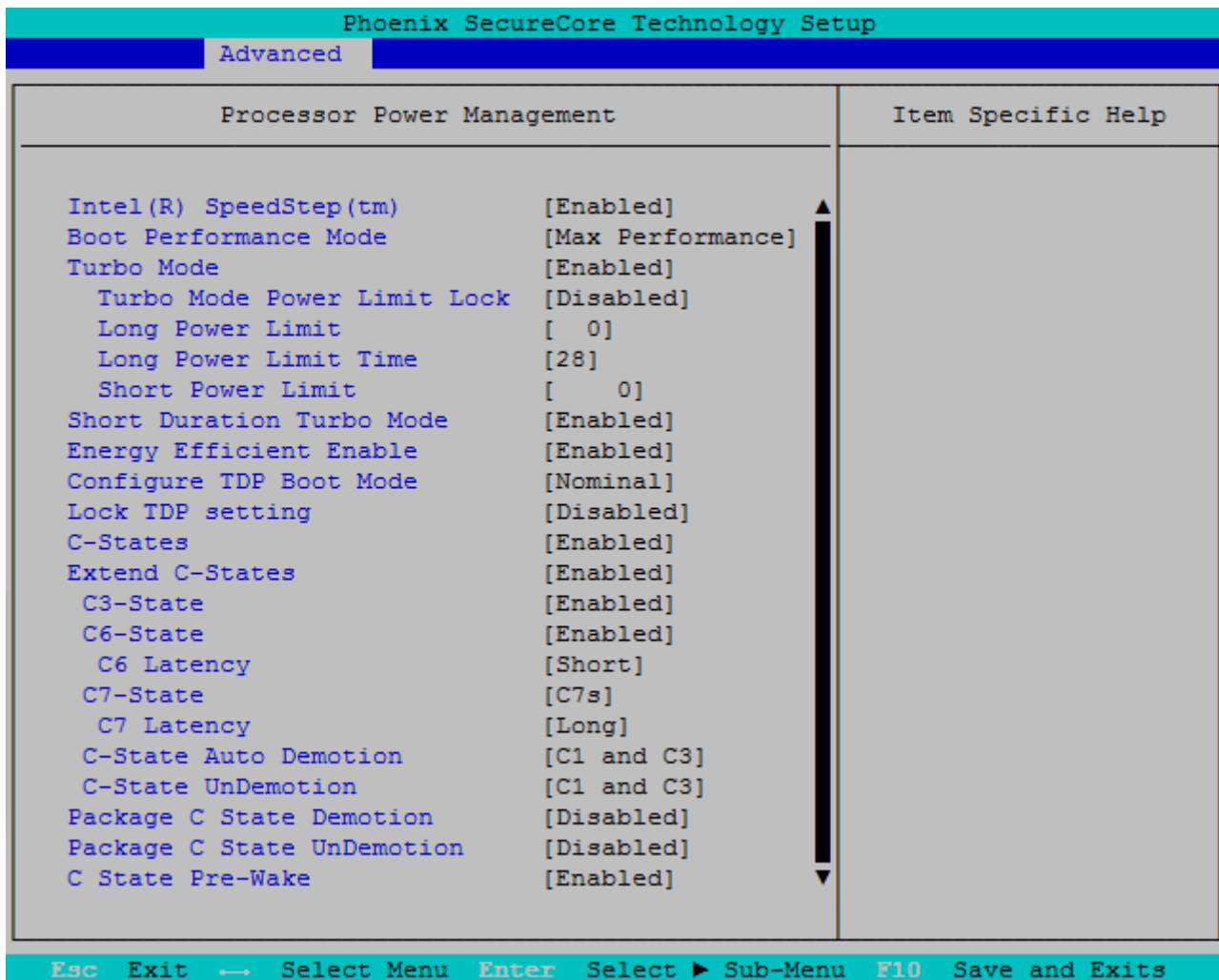


Processor Configuration



Feature	Options	Description
Active Processor Cores	All 1 2 3	Number of cores to enable in each processor package
Intel® HT Technology	Enabled Disabled	When Disabled only one thread per enabled core is enabled
CPU Flex Ratio Override	Disabled Enabled	Enable/Disable CPU Flex Ratio Programming. If Disabled, CPU frequency is set to maximum Ratio automatically
- CPU Flex Ratio Settings	24	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	Enabled Disabled	Enables/Disables 'Execute Disable functionality', also known as Data Execution Prevention DEP
Intel® Virtualization Technology	Disabled Enabled	When enabled, a VMM can utilize the additional hardware capabilities
Intel® Trusted Execution Technology	Disabled Enabled	Enable/Disable Intel TXT (enabled only in customized BIOS versions)

Processor Power Management



Feature	Options	Description
Intel® SpeedStep(TM)	Enabled Disabled	Enable/Disable processor performance states (P-States)
Boot Performance Mode	Max Performance Max Battery Auto	Select the performance state that the BIOS sets before OS hand-off
Turbo Mode	Enabled Disabled	Enable processor Turbo Mode
- Turbo Mode Power Limit Lock	Disabled 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 Disabled	Enable/Disable Short Duration Turbo Mode for processor
- Energy Efficient Enable	Enabled Disabled	Enable/Disable Energy Efficient for processor
Configure TDP Boot Mode	Nominal Down Up Disabled	Configure TDP Mode (cTDP). Disabled option will skip all cTDP boot configurations

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

Miscellaneous

Phoenix SecureCore Technology Setup

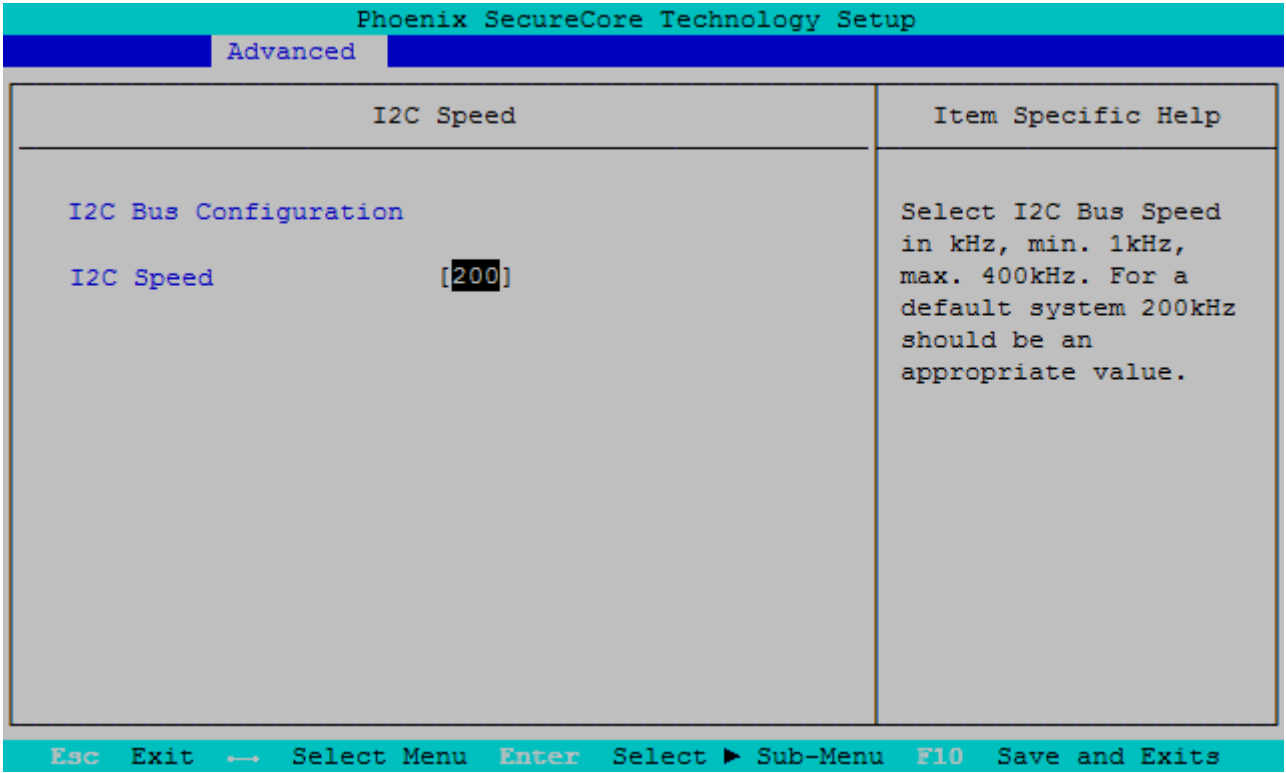
Advanced

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

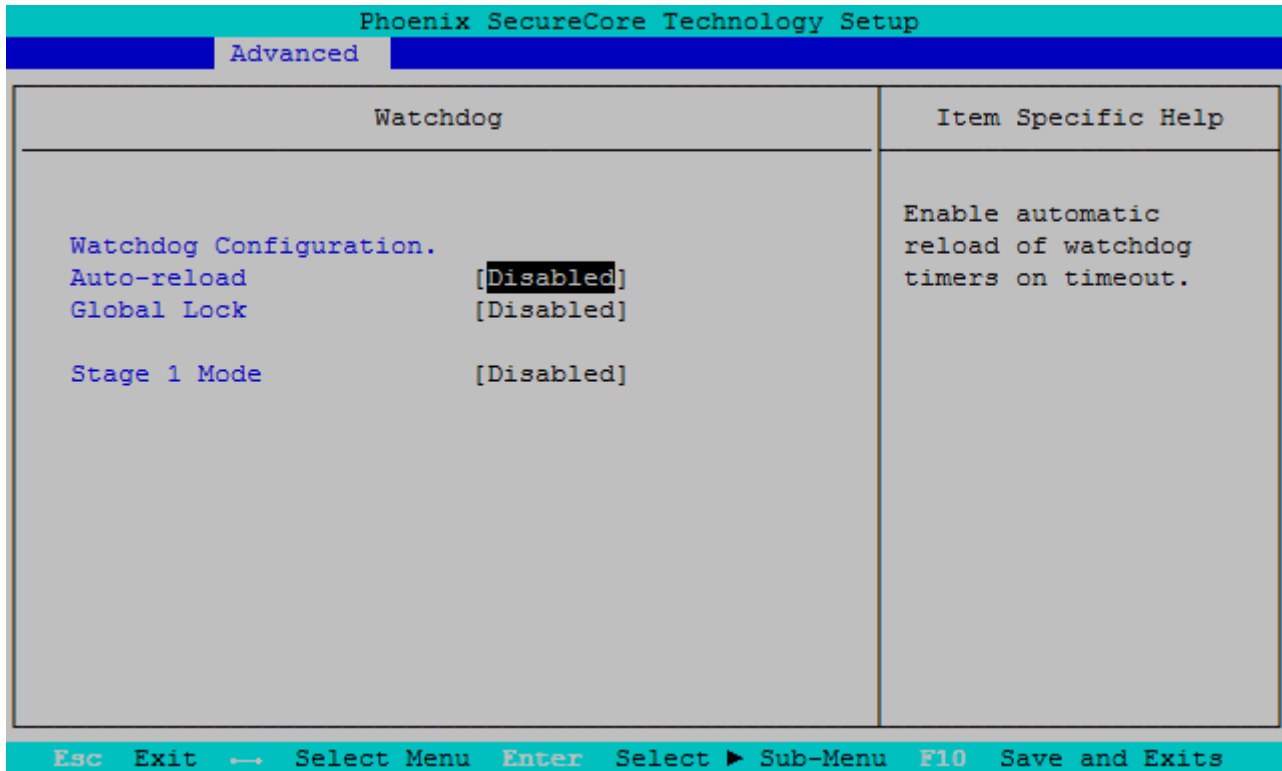
Feature	Options	Description
S5 Eco	Disabled Enabled	Enable/Disable Kontron S5 Eco mode. Reduces supply current in Soft Off (S5) to less than 1mA. If enabled, power button is the only wake-up source in S5! See chapter S5 Eco for further details
Smart Battery Configuration	Disabled Auto Charger Manager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

I2C Speed



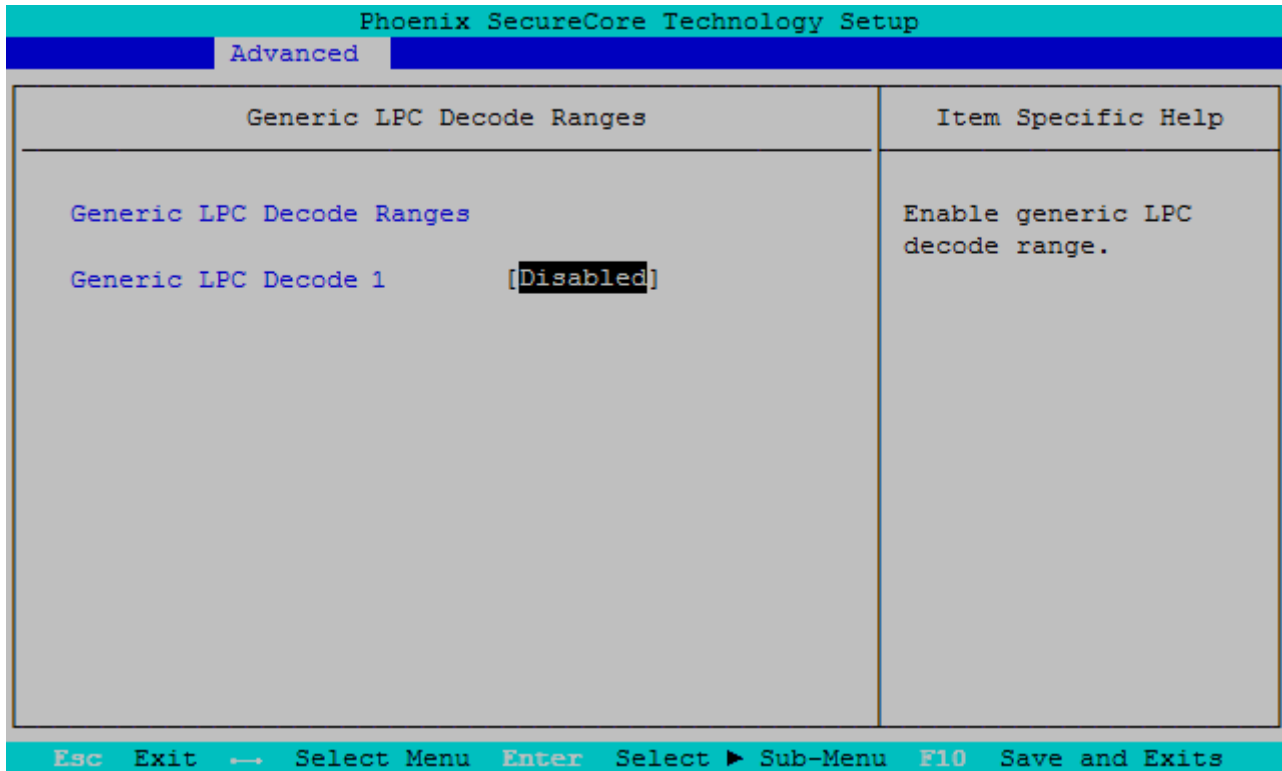
Feature	Options	Description
I2C Speed	200	Select I2C Bus Speed in kHz from 1kHz to 400kHz

Watchdog



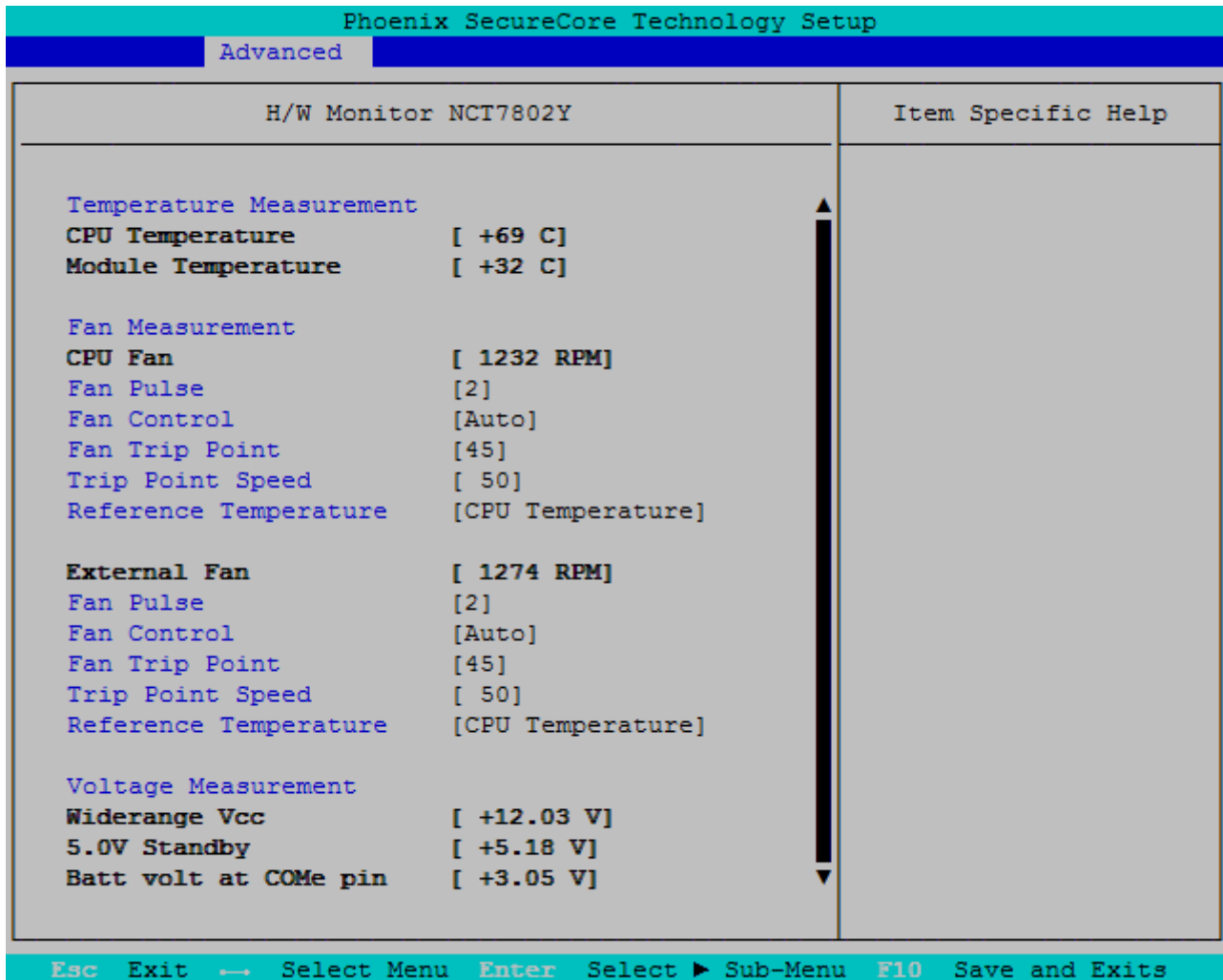
Feature	Options	Description
Auto-reload	Disabled Enabled	Enable automatic reload of watchdog timers on timeout
Global Lock	Disabled Enabled	If set to enabled, all Watchdog registers (except WD_KICK) become read only until the board is reset
Stage 1 Mode	Disabled Reset NMI SCI	Select Action for first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

Generic LPC Decode Ranges



Feature	Options	Description
Generic LPC Decode 1	Disabled 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 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 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



Feature	Value/Options	Description
CPU Temperature	xx°C	Shows the measured temperature of the CPU Diode with onboard HWM
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 Manual Auto	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	CPU Temperature PCH Temperature 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 Manual Auto	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 Module Temperature CPU Temperature	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

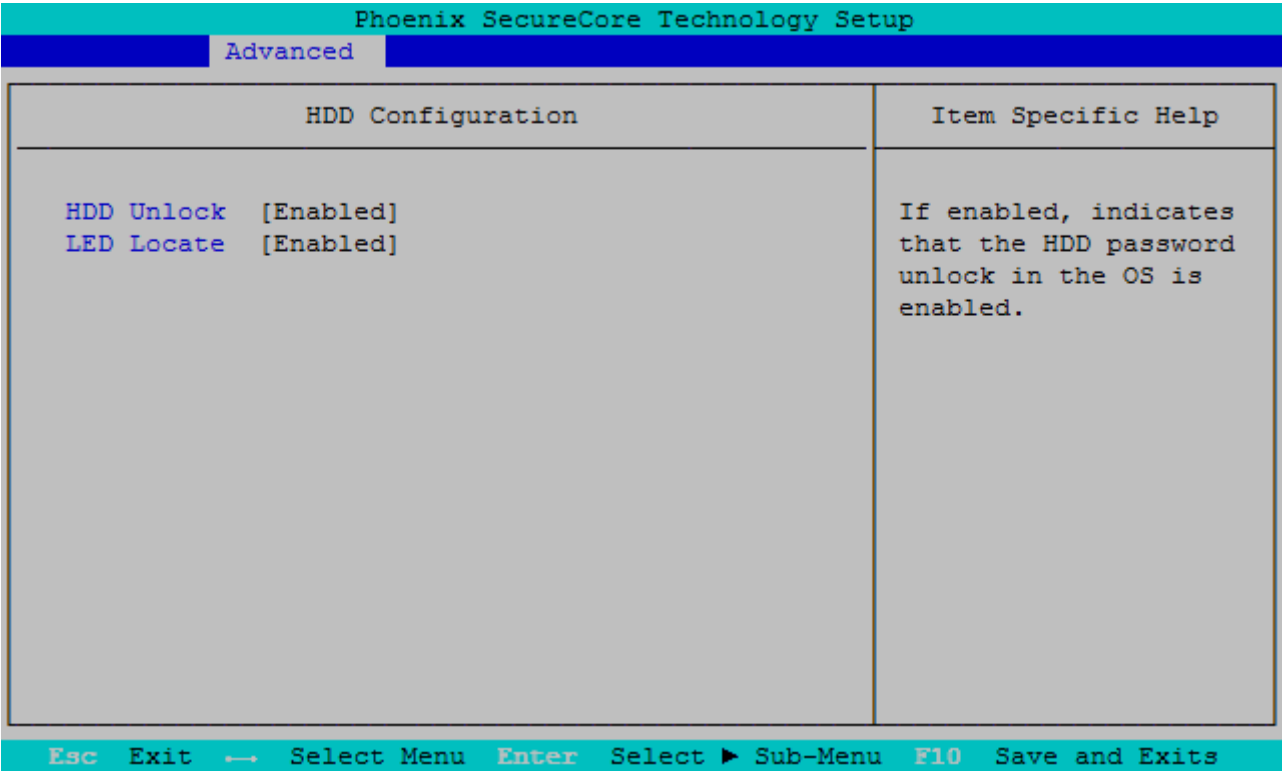
Phoenix SecureCore Technology Setup	
Advanced	
HDD Configuration	Item Specific Help
SATA Device	[Enabled]
Interface Combination	[AHCI]
Aggressive Link Power	[Enabled]
SATA Speed	[Gen. 2]
► Software Feature Mask Configuration	
ComExpress SATA 0	Not Installed or the po
Port Enable	[Enabled]
Hot Plug	[Disabled]
SATA Device Type	[Hard Disk Drive]
DevSlp	[Disabled]
DITO Configuration	[Disabled]
DITO Value	[625]
DITO Multiplier Value	[15]
ComExpress SATA 1	Not Installed or the po
Port Enable	[Enabled]
Hot Plug	[Disabled]
SATA Device Type	[Hard Disk Drive]
DevSlp	[Disabled]
DITO Configuration	[Disabled]
DITO Value	[625]
DITO Multiplier Value	[15]
ComExpress SATA 2	Not Installed or the po
Port Enable	[Enabled]
Hot Plug	[Disabled]
SATA Device Type	[Hard Disk Drive]
DevSlp	[Disabled]
DITO Configuration	[Disabled]
DITO Value	[625]
DITO Multiplier Value	[15]
ComExpress SATA 3	Not Installed or the po
Port Enable	[Enabled]
Hot Plug	[Disabled]
SATA Device Type	[Hard Disk Drive]
DevSlp	[Disabled]
DITO Configuration	[Disabled]
DITO Value	[625]
DITO Multiplier Value	[15]

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

Feature	Options	Description
SATA Device	Enabled Disabled	Enable/Disable SATA Device
Interface Combination	IDE AHCI RAID	Select the SATA controllers operation mode
Aggressive Link Power	Disabled Enabled	If enabled, turns on Aggressive Link Power Management on all HDD ports
SATA Speed	Gen1 Gen2 Gen3	Select the supported SATA speed mode
Port Enable	Enabled Disabled	Enable or Disable SATA Port
Hot Plug	Disabled	Designates this port as Hot Pluggable. Requires

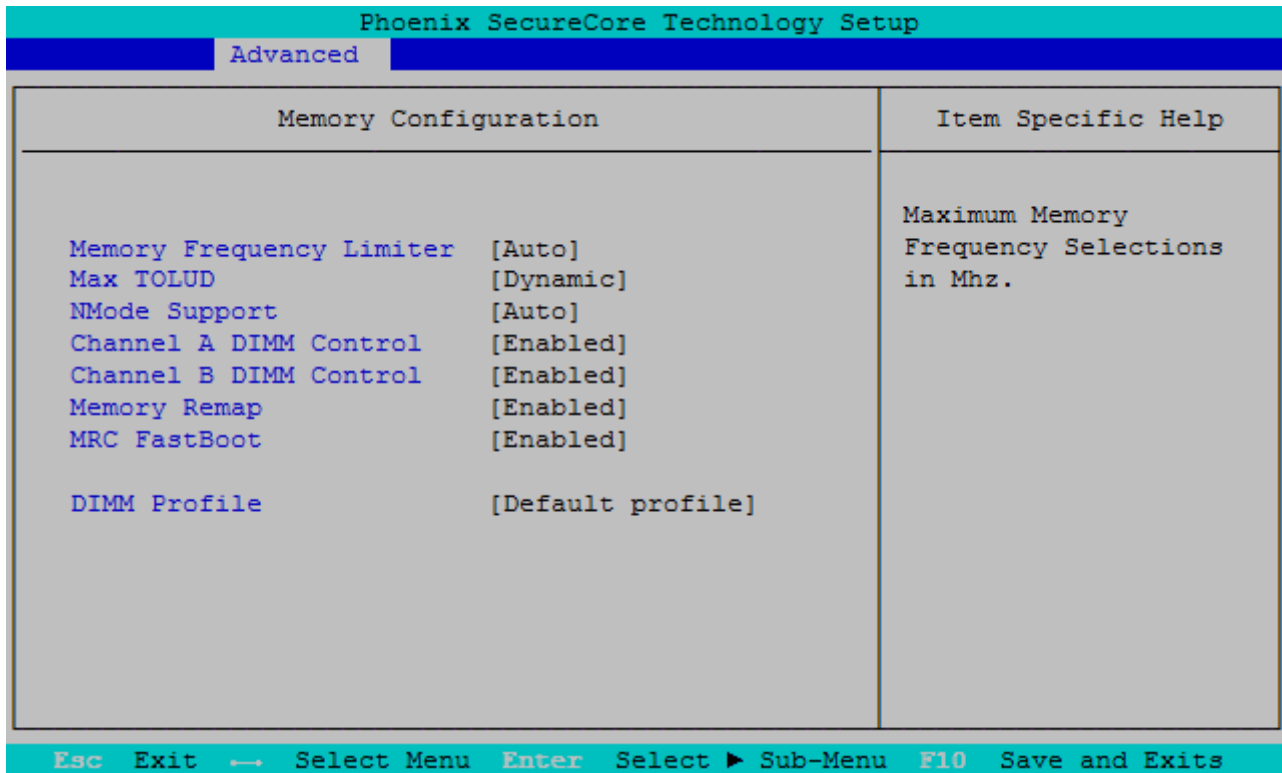
	Enabled	hardware support
SATA Device Type	Hard Disk Drive Solid State Drive	Identify the SATA port is connected to Solid State Drive or Hard Disk Drive
DevSlp	Disabled Enabled	RTD3 Device Sleep Support
DITO Configuration	Disabled Enabled	Enable/Disable Device Sleep Idle Timeout Configuration
DITO Value	625	The Host computes the total idle timeout as a product of DITO Multiplier and Dito Value: DITO actual = DITO + (DM+1)
DITO Multiplier Value	15	The Host computes the total idle timeout as a product of DITO Multiplier and Dito Value: DITO actual = DITO + (DM+1)

Software Feature Mask Configuration



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

Memory Configuration



Feature	Options	Description
Memory Frequency Limiter	Auto 2067 1333 1600 1867 2133 2400 2667	Select the memory frequency in MHz
Max TOLUD	Dynamic 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	Auto 1N Mode 2N Mode	Select the memory supported Command Rate (N-Mode)
Channel A DIMM Control	Enabled Disabled	Enables or disables DIMMs on channel A
Channel B DIMM Control	Enabled Disabled	Enables or disables DIMMs on channel B
Memory Remap	Enabled Disabled	Enable/Disable Memory Remap above 4GB
MRC FastBoot	Enabled Disabled	Enable/Disable MRC FastBoot. Generally, this option only takes effect when doing cold boots/resets
DIMM Profile	Default DIMM profile XMP profile 1 XMP Profile 2	Select Intel Extreme Memory Profile XMP if supported by DIMM SPD

System Agent (SA) Configuration

Phoenix SecureCore Technology Setup

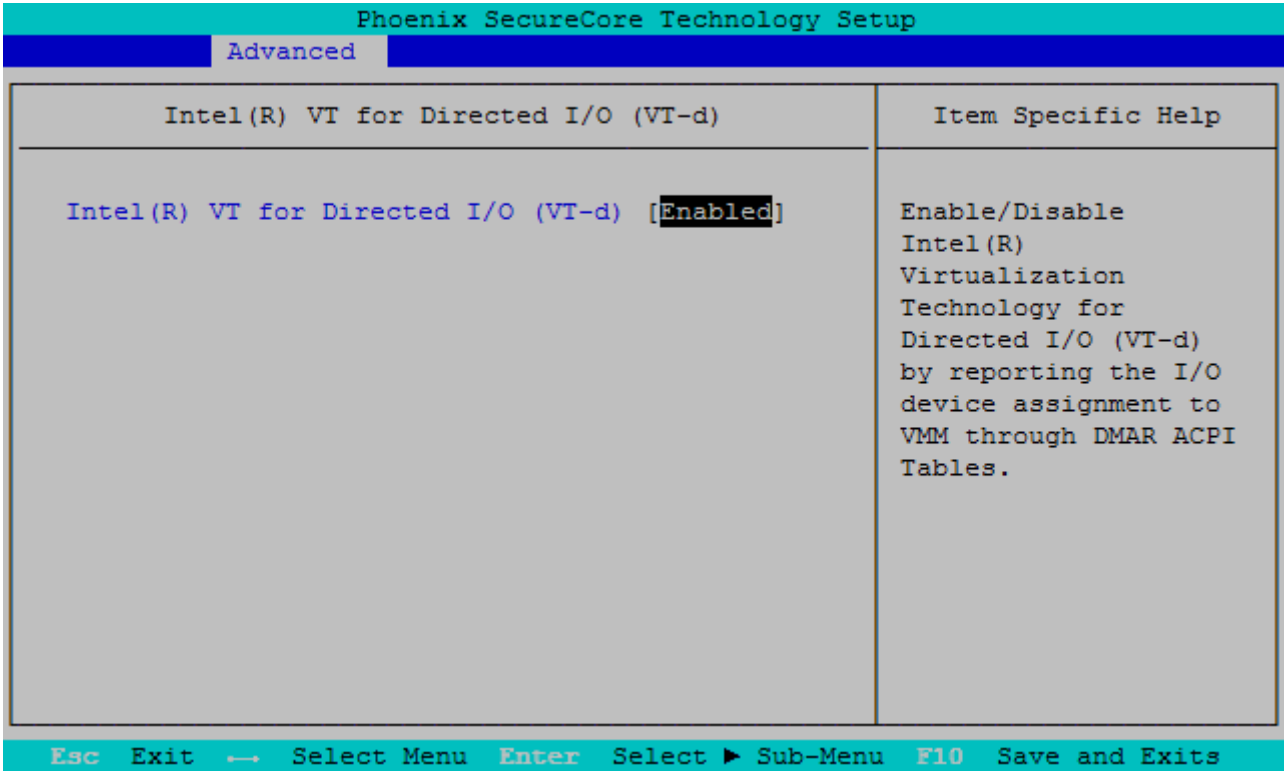
Advanced

System Agent (SA) Configuration	Item Specific Help
▶ Intel(R) VT for Directed I/O (VT-d) ▶ Graphics Configuration Cpu Audio Device (D0:D3:F0) [Enabled]	

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

Feature	Options	Description
CPU Audio Device (D0:D3:F0)	Enabled 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 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

Phoenix SecureCore Technology Setup	
Advanced	
Graphics Configuration	Item Specific Help
Graphics Turbo IMON Current [31]	
Primary Display Selection [Auto]	
Internal Graphics [Auto]	
GTT Size [2MB]	
Aperture Size [256MB]	
DVMT Pre-Allocated [32MB]	
DVMT Total Gfx Mem [256MB]	
Gfx Low Power Mode [Enabled]	
► IGD Configuration	

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

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

IGD Configuration

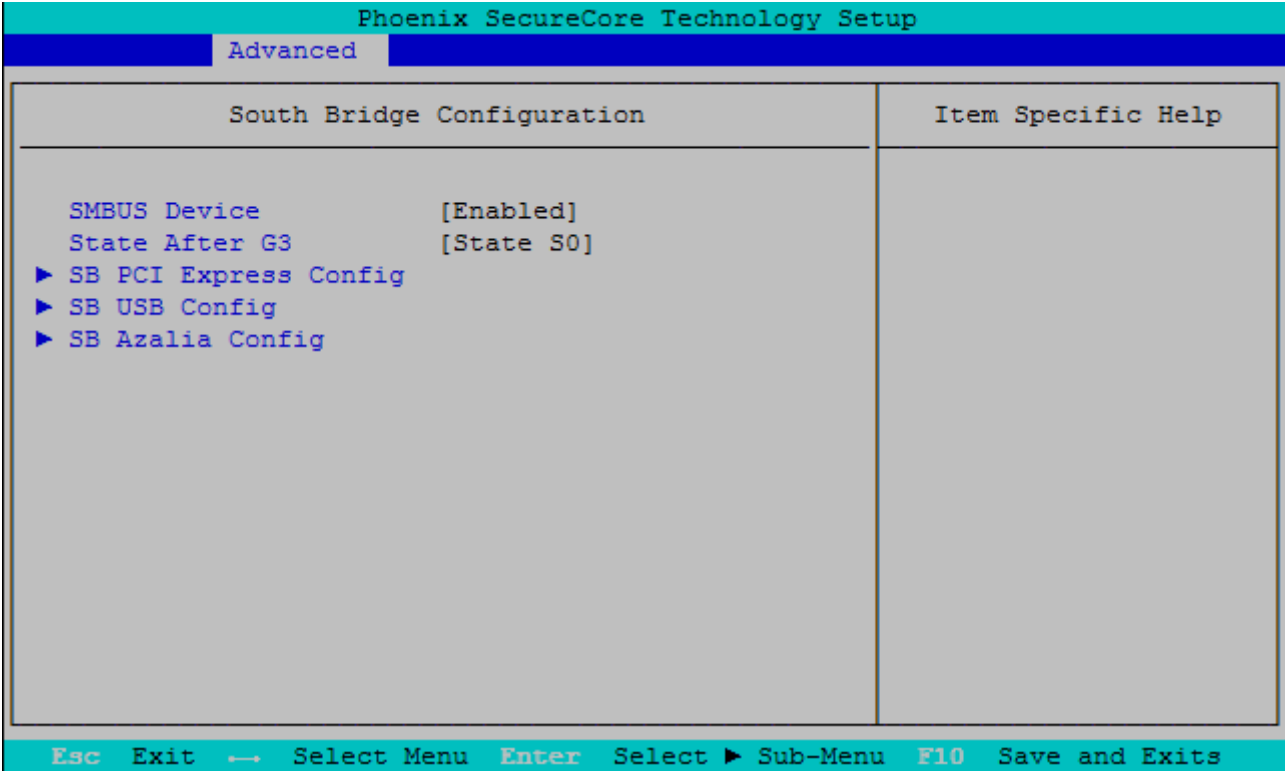
Phoenix SecureCore Technology Setup		
Advanced		
IGD Configuration		Item Specific Help
IGD managed by: Legacy Video BIOS [2175]		Select the Video Device activated during POST. This has no effect if external graphics are present.
IGD - Boot Type	[Auto]	
Backlight Control	[I2C]	
Backlight Value	[128]	
eDP Panel Type	[LVDS]	
LVDS Clock Center Spreading	[No Spreading]	
EFP1 Type	[DP with HDMI/DVI]	
EFP2 Type	[DP with HDMI/DVI]	
Mode Persistence	[Disabled]	

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

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

EFP2 Type	DP with HDMI/DVI DP with DVI HDMI/DVI	External Connectors
Mode Persistence	Disabled Enabled	Enables/Disables Mode Persistence

South Bridge Configuration



Feature	Options	Description
SMBUS Device	Disabled Enabled	Enable/Disable SMBUS Device
State After G3	State S5 State S0 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

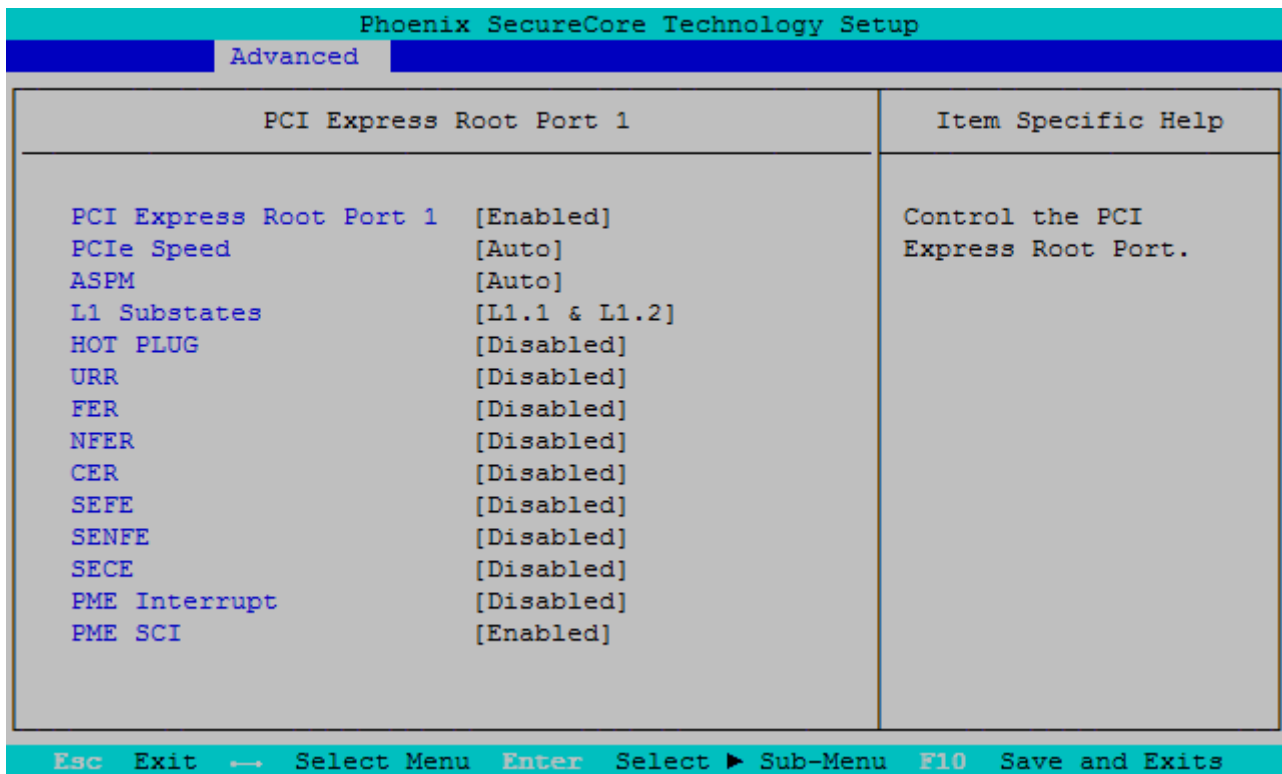
SB PCI Express Config

Phoenix SecureCore Technology Setup		
Advanced		
SB PCI Express Config	Item Specific Help	
DMI Link ASPM Control	[Enabled]	Enabled or Disabled PCI Express Root Port Clock Gating.
DMI Link Extended Synch Control	[LOS]	
PCI Express port assigned to LAN	[Disabled]	
5		
▶ PCI Express Port 1 Config		
▶ PCI Express Port 2 Config		
▶ PCI Express Port 3 Config		
▶ PCI Express Port 4 Config		
PCI ExpressCard 0	[Disabled]	
PCI ExpressCard 1	[Disabled]	

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

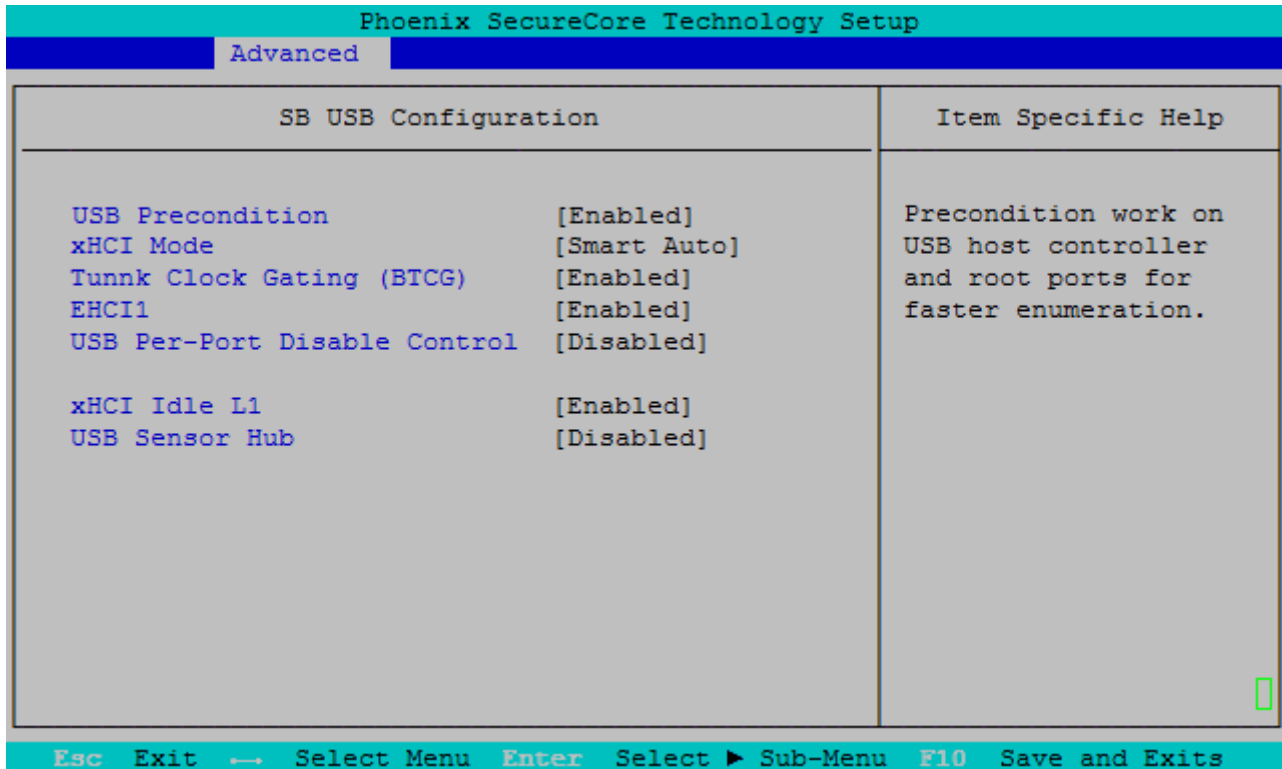
Feature	Options	Description
PCIe Root Port Clock Gating	Disabled Enabled	Enable or Disable PCI Express Clock Gating for each root port
DMI Link ASPM Control	Disabled Enabled	Controls Active State Power Management on both NB side and SB side of the DMI Link
DMI Link Ext Synch	Disabled Enabled	Controls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

PCI Express Root Port 1/2/3/4



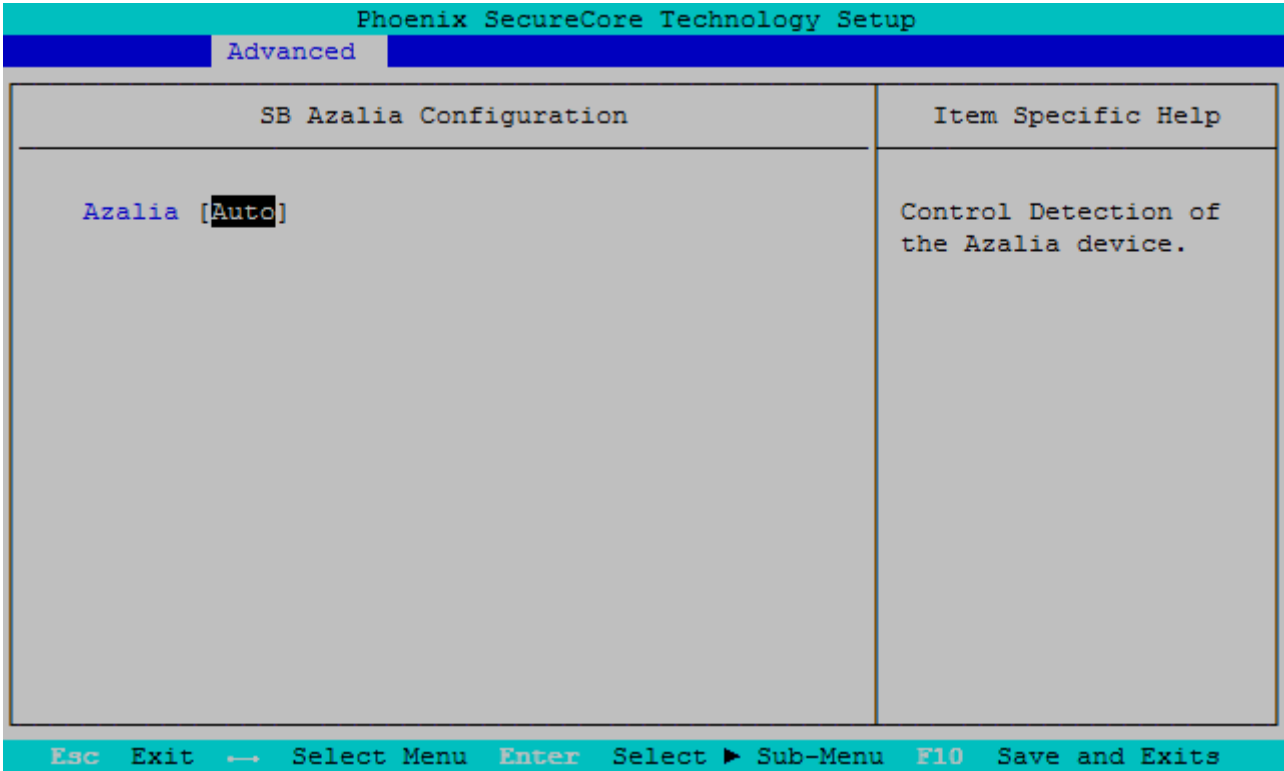
Feature	Options	Description
PCI Express Root Port #	Disabled Enabled	Control the PCI Express Root Port
PCIe Speed	Auto Gen1 Gen2	Select PCIe Speed to Gen1 or Gen2
ASPM	Disabled LOs L1 LOs and L1 Auto	Control PCIe Active State Power Management settings
L1 Substates	Disabled L1.1 L1.2 L1.1 & L1.2	PCI Express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

SB USB Config



Feature	Options	Description
USB Precondition	Disabled Enabled	Precondition work on USB host controller and root ports for faster enumeration
xHCI Mode	Disabled Enabled Auto Smart Auto	Mode of operation of xHCI controller
Trunk Clock Gating (BTCG)	Disabled Enabled	Enable/Disable BTCG
EHCI1	Disabled Enabled	Control the USB EHCI (USB2.0) functions
USB Per-Port Disable Control	Disabled Enabled	Controls each of the USB ports (0~13)
- USB Port #0 Enable/Disable - USB Port #1 Enable/Disable - USB Port #2 Enable/Disable - USB Port #3 Enable/Disable - USB Port #4 Enable/Disable - USB Port #5 Enable/Disable - USB Port #6 Enable/Disable - USB Port #7 Enable/Disable	Disabled Enabled	Enable/Disable USB port
xHCI Idle L1	Disabled Enabled	Enable/Disable xHCI Idle L1
USB Sensor Hub	Disabled Enabled	Enable/Disable USB Sensor Hub

SB Azalia Config



Feature	Options	Description
Azalia	Disabled 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] LAN OPROM Selection [Onboard only] Wake on PCH LAN [Enabled] ASF Support [Enabled]	Enable/Disable PCH Internal LAN.

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

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

CPLD Configuration

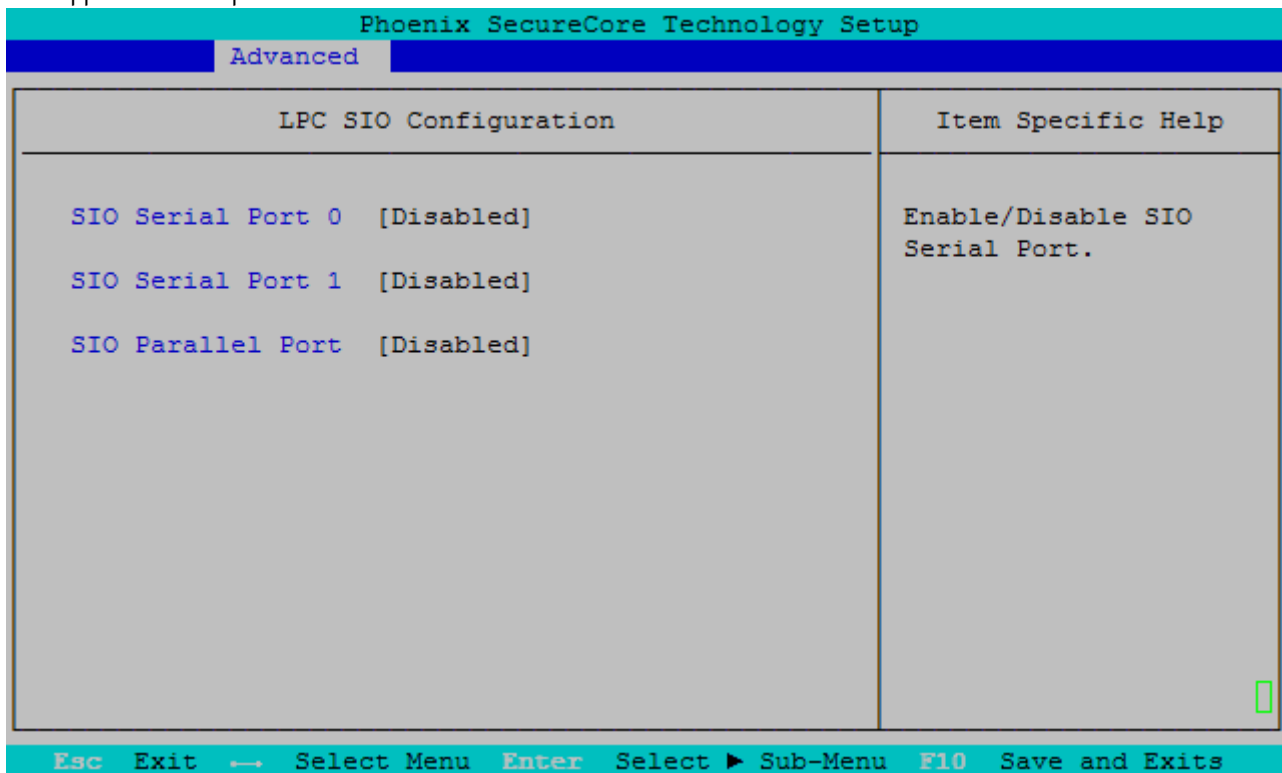
Phoenix SecureCore Technology Setup		
Advanced		
CPLD configuration		Item Specific Help
Serial Port 0	[Enabled]	Enable/Disable Serial Port.
Base Address	[3F8]	
IRQ	[4]	
Serial Port 1	[Enabled]	
Base Address	[2F8]	
IRQ	[3]	
GPIO IRQ	[Disabled]	
I2C IRQ	[Disabled]	

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

Feature	Options	Description
Serial Port 0	Disabled Enabled	Enable or Disable Serial Port (COM) 0
Base Address	3F8 2F8 3E8 2E8	Configure Serial Port Base Address
IRQ	3 4 5 6 7 12	Configure Serial Port IRQ
Serial Port 1	Disabled Enabled	Enable or Disable Serial Port (COM) 1
Base Address	3F8 2F8 3E8 2E8	Configure Serial Port Base Address
IRQ	3 4 5 6 7 12	Configure Serial Port IRQ
GPIO IRQ	Disabled 14 15	Configure IRQ for GPIO pins
I2C IRQ	Disabled 14 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-CHL6 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	Disabled Enabled	Enable or Disable SIO Serial Port
- Base Address	3F8 2F8 3E8 2E8	Configure Serial Port Base Address
- IRQ	3 4 5 6 7 12	Configure Serial Port IRQ
Serial Port 1	Disabled Enabled	Enable or Disable SIO Serial Port
- Base Address	3F8 2F8 3E8 2E8	Configure Serial Port Base Address
- IRQ	3 4 5 6 7 12	Configure Serial Port IRQ
SIO Parallel Port	Disabled Enabled	Enable or Disable SIO Parallel Port
- Device Mode	Standard Parallel Port EPP ECP & EPP 1.9 ECP & EPP 1.7	Configure Parallel Port Mode
- Base Address	378 278 3BC	Configure Parallel Port Base Address

ME Configuration

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

Thermal Configuration

Phoenix SecureCore Technology Setup	
Advanced	
Thermal Configuration	Item Specific Help
▶ CPU Thermal Configuration ▶ Platform Thermal Configuration	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

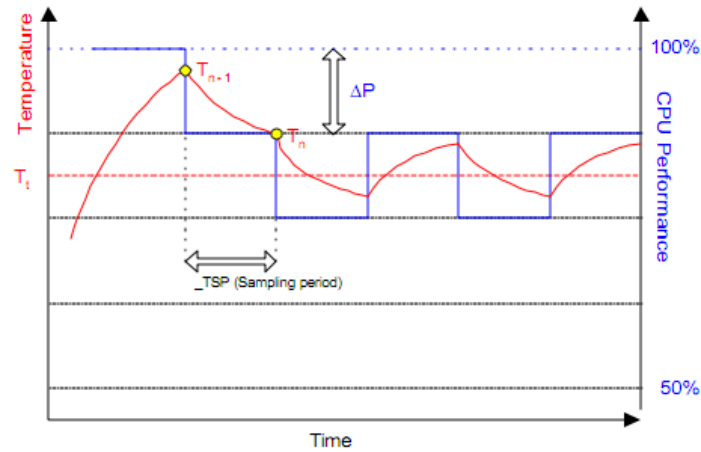
Feature	Options	Description
Thermal Monitor	Disabled Enabled	Enable processor Thermal Monitor thermal control. Requires GV3
Bi-directional PROCHOT#	Disabled Enabled	When a processor thermal sensor trips (either core), the PROCHOT# is driven. If bi-direction is enabled, external agents can drive PROCHOT# to throttle the processor
PROCHOT# OUT	Disabled Enabled	If Bi-directional PROCHOT# is enabled, PROCHOT# OUT can be disabled selectively
PROCHOT# Response	Disabled Enabled	Enable/Disable PROCHOT Response
DTS	Disabled Enabled	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]	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	[90 C]	
Passive TC1 Value	[1]	
Passive TC2 Value	[5]	
Passive TSP Value	[10]	
Esc Exit → Select Menu Enter Select ► Sub-Menu F10 Save and Exits		

Feature	Options	Description
Critical Trip Point	POR 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 ... 90°C 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	1	This value sets the TC1 value for the ACPI Passive Cooling Formula. Range 1 - 16
- Passive TC2 Value	5	This value sets the TC2 value for the ACPI Passive Cooling Formula. Range 1 - 16
- Passive TSP Value	10	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

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

ΔP 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) 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.
Clock Manipulation [ICC Failure]	
ICC Overclocking Library [9.0.0.1209]	
► Clock 2	

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

Feature	Options	Description
Use Watchdog Timer for ICC	Disabled 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 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 2

Phoenix SecureCore Technology Setup

Advanced

Clock 2

Item Specific Help

PCI33, SATA, USB3

Maximum supported frequency [100.0 MHz]

Minimum supported frequency [100.0 MHz]

Current frequency [100.0 MHz]

New frequency [10KHz] [10000]

Supported SSC modes [down]

Current SSC mode [down]

New SSC mode [down]

Maximum supported SSC % [0.50]

Current SSC % [0.50]

New SSC spread percent [0.01%] [50]

▲

Spread Spectrum Clocking mode.

Determines method of clock spectrum distribution around base frequency.

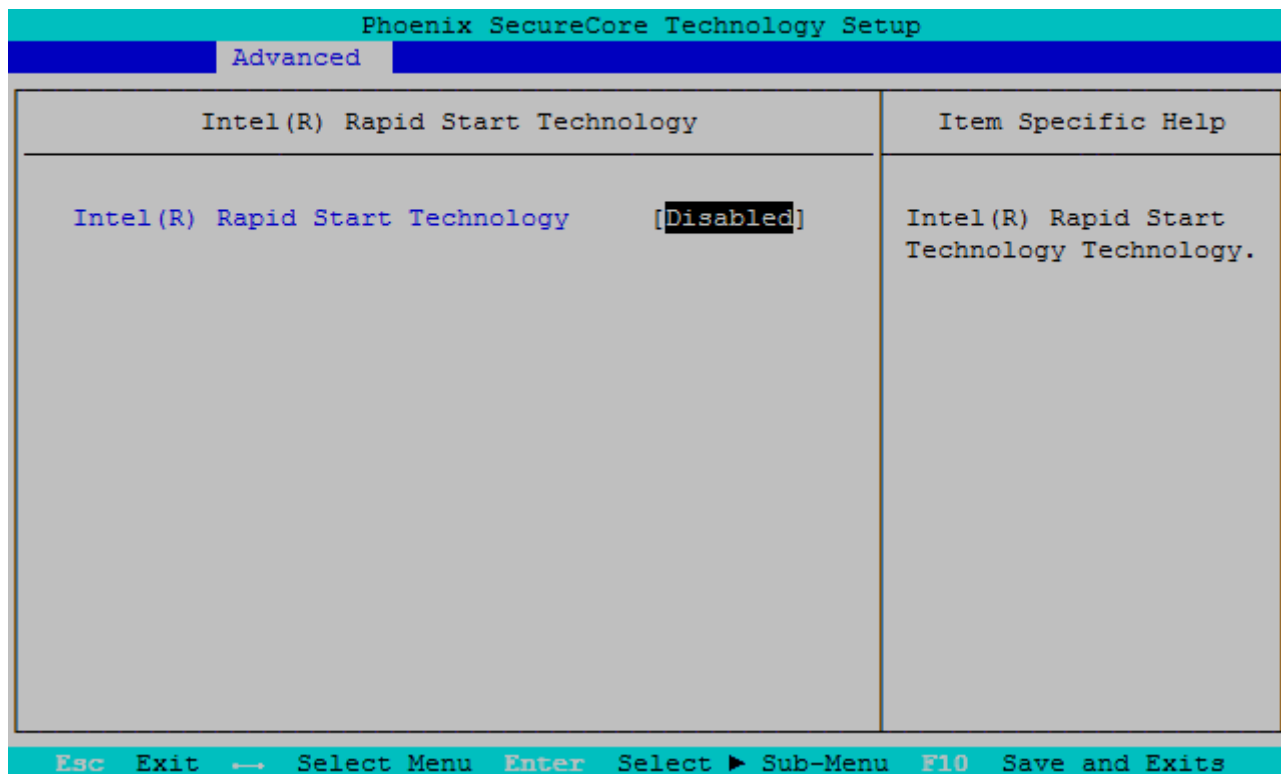
Changes will not be applied unless 'Apply setting' is pressed.

▼

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

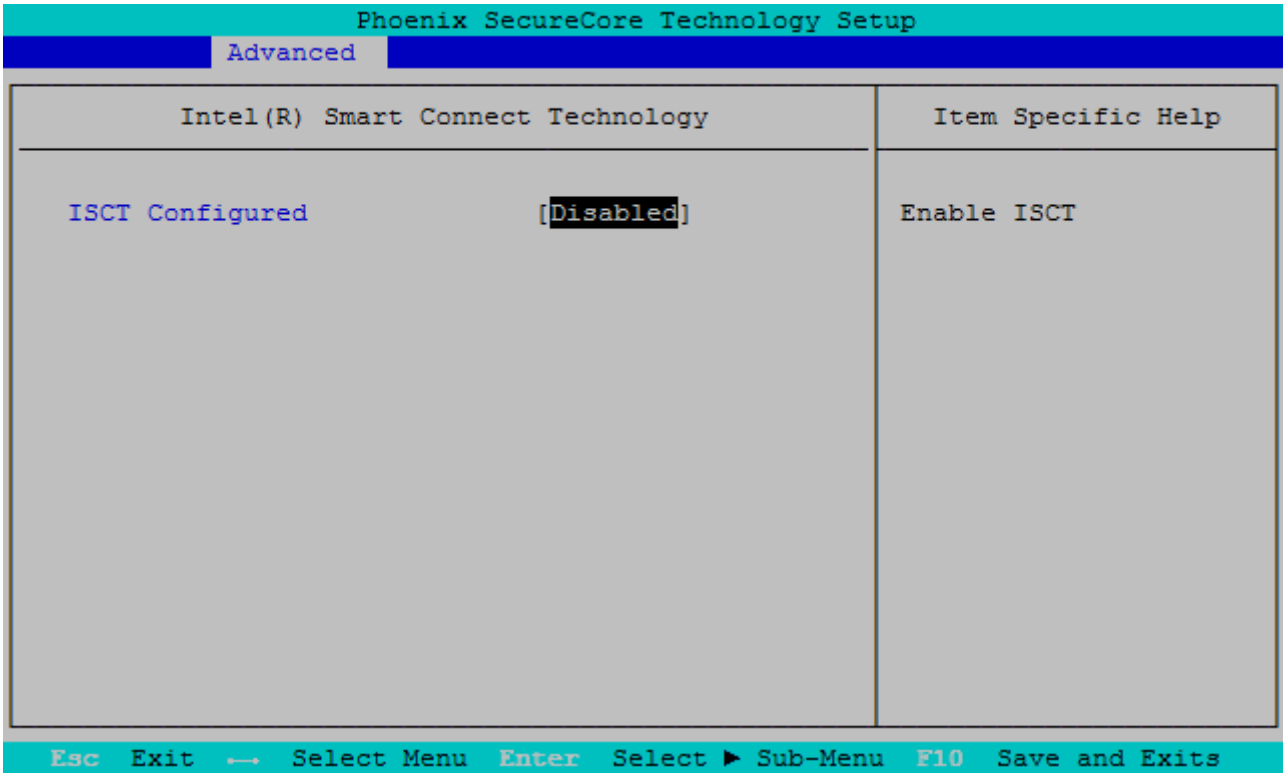
Feature	Options	Description
New SSC spread percent	50	Clock spectrum spread in 0.01% increments. Determines spectrum deviation away from base frequency. Allowed range is limited by Max supported SSC%.

Intel® Rapid Start Technology



Feature	Options	Description
Intel® Rapid Start Technology Support	Disabled Enabled	Enable/Disable Intel® Rapid Start Technology
- Entry on S3 RTC wake	Disabled Enabled	Intel® Rapid Start Technology invocation upon S3 RTC wake
- Entry after	Immediately 1 minute 2 minutes 5 minutes 10 minutes 15 minutes 30 minutes 1 hour 2 hours	RTC wake timer at S3 entry
- Display Save Restore	Disabled 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 Enabled	Enable Intel® Smart Connect Technology
ISCT Notification Control	Disabled Enabled	Enable ISCT Notification Control
ISCT WLAN Power Control	Disabled Enabled	Enable ISCT WLAN Power Control
ISCT WWAN Power Control	Disabled Enabled	Enable ISCT WWAN Power Control
ISCT SASD Format Control	Actual Time Sleep Duration	Select ISCT wake time format for ACPI SASD method. Actual Time: -YYMMDDHHMMSS Sleep Duration: - Duration in seconds

8.5.3 Security

Phoenix SecureCore Technology Setup

MainAdvancedSecurityBootExit

Supervisor Password is: Cleared

User Password is: Cleared

Set Supervisor Password [Enter]

Supervisor Hint String []

Set User Password [Enter]

User Hint String []

Min. password length [1]

Authenticate User on Boot [Disabled]

HDD Security Status

No HDD detected

Trusted Platform Module (TPM)

TPM Support [Enabled]

▶ TPM Configuration

Item Specific Help

Set or clear the Supervisor account's password.

EscExit↔Select MenuEnterSelect▶Sub-MenuF10Save and Exits

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 Enabled	This is used to decide whether TPM support should be enabled or disabled

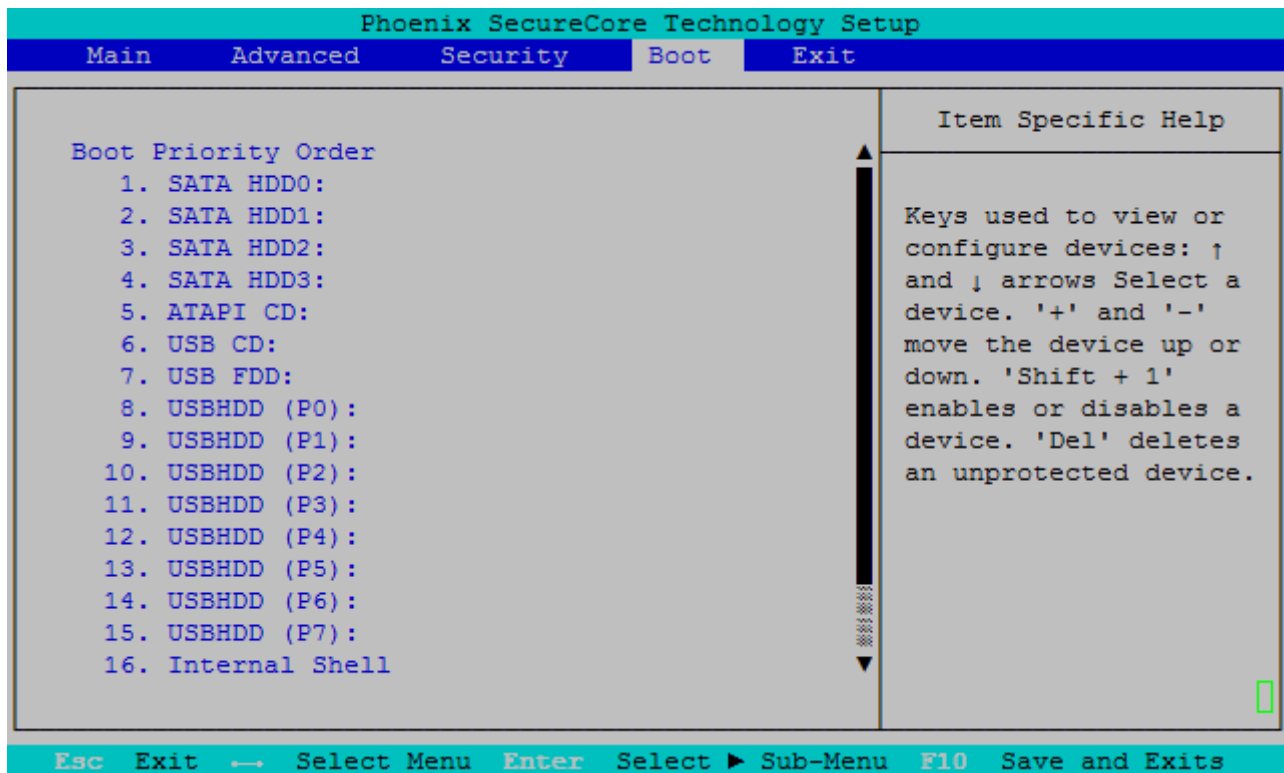
Security

Phoenix SecureCore Technology Setup		
Security		
TPM Configuration		Item Specific Help
Current TPM State	[Enabled and Activated]	Enact TPM Action. Note: Most TPM actions require TPM to be Enabled to take effect.
TPM Action	[No Change]	
Omit Boot Measurements	[Disabled]	

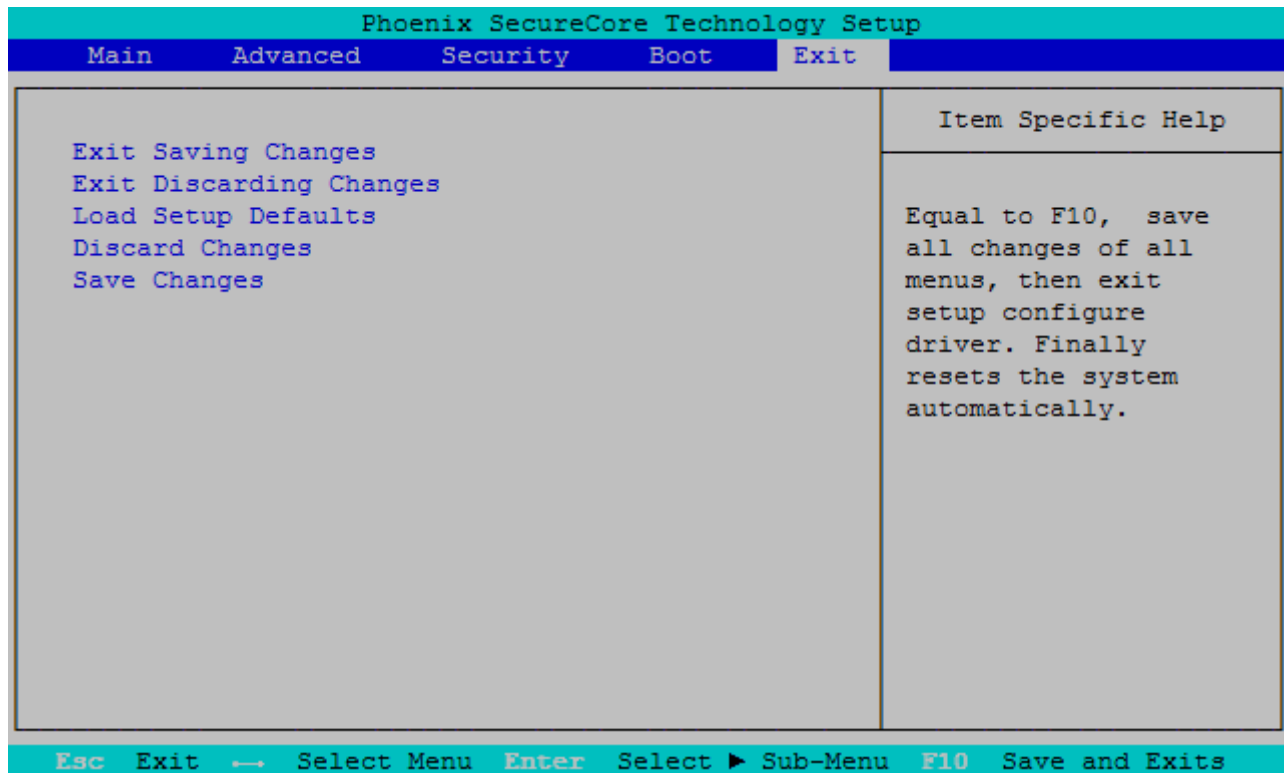
Esc Exit → Select Menu Enter Select ► Sub-Menu F10 Save and Exits

Feature	Options	Description
TPM Action	No Change Enable Disable Activate Deactivate Clear Enable and Activate Disable and Deactivate Set Owner Install, with state=True Set Owner Install, with state=False Enable, Activate, and Set Owner Install with state=True Disable, Deactivate, and Set Owner Install with state=False Clear, Enable, and Activate Require PP for provisioning Do not require PP for provisioning Require PP for clear Do not require PP for clear Enable, Activate, and clear Enable, Activate, Clear, Enable, and Activate	Enact TPM Action
Omit Boot Measurements	Disabled Enabled	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

Europe, Middle East & Africa	North America	Asia Pacific	
Oskar-von-Miller-Str. 1 85386 Eching/Munich Germany Tel.: +49 (0)8165/ 77 777 Fax: +49 (0)8165/ 77 219 info@kontron.com	14118 Stowe Drive Poway, CA 92064-7147 USA Tel.: +1 888 294 4558 Fax: +1 858 677 0898 info@us.kontron.com	17 Building,Block #1,ABP. 188 Southern West 4th Ring Beijing 100070, P.R.China Tel.: + 86 10 63751188 Fax: + 86 10 83682438 info@kontron.cn	