



SMARC-sXBTi

Document Revision 1.1

» Table of Contents «

1	User Information.....	5
1.1	About This Document.....	5
1.2	Copyright Notice.....	5
1.3	Trademarks.....	5
1.4	Standards.....	5
1.5	Warranty.....	6
1.6	Technical Support.....	6
2	Introduction.....	7
2.1	Product Description.....	7
2.2	SMARC™ Computer-on-Modules.....	7
3	Product Specification.....	8
3.1	Modules & Accessories.....	8
3.2	Functional Specification.....	10
3.3	Block Diagram.....	13
3.4	Electrical Specification.....	14
3.4.1	Supply Voltage.....	14
3.4.2	Power Supply Rise Time.....	14
3.4.3	Supply Voltage Ripple.....	14
3.5	Power Control.....	15
3.6	Environmental Specification.....	16
3.6.1	Temperature Specification.....	16
3.6.2	Humidity.....	16
3.7	Standards and Certifications.....	17
3.8	MTBF.....	18
3.9	Mechanical Specification.....	19
3.9.1	Module Dimension.....	19
3.9.2	Height on Top.....	19
3.9.3	Height on Bottom.....	19
3.9.4	Mechanical Drawing.....	19
3.10	Module Dimensions.....	20
3.11	Thermal Management, Heatspreader and Cooling Solutions.....	21
4	Features and Interfaces.....	22
4.1	Onboard eMMC Flash.....	22
4.2	S5 Eco Mode.....	22
4.3	Speedstep Technology.....	23
4.4	C-States.....	24
4.5	Camera Interfaces.....	25
4.6	Graphics Features.....	26
4.7	ACPI Suspend Modes and Resume Events.....	27

5	System Resources.....	28
5.1	Interrupt Request (IRQ) Lines.....	28
5.2	Memory Area.....	28
5.3	I/O Address Map.....	29
5.4	Peripheral Component Interconnect (PCI) Devices.....	30
5.5	LPC addresses.....	30
5.6	I2C Bus.....	30
5.7	System Management (SM) Bus.....	31
6	Connectors.....	32
6.1	SMARC™ Connector Top Side.....	32
6.2	SMARC™ Connector Bottom Side.....	35
7	BIOS Operation.....	38
7.1	Determining the BIOS Version.....	38
7.2	BIOS Update.....	38
7.3	POST Codes.....	38
7.4	Setup Guide.....	38
7.5	BIOS Setup.....	40
7.5.1	Main.....	40
7.5.2	Advanced.....	44
7.5.3	Security.....	63
7.5.4	Boot.....	65
7.5.5	Exit.....	66

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 © 2003-2015 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-I/O® 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.

2 Introduction

2.1 Product Description

The new Kontron SMARC-sXBTi Computer-on-Modules has been developed to comply with the SGET specification and is equipped with Intel® Atom™ processor E3800 series and up to 8 GB RAM, optional with ECC. They support the extended temperature range of -40°C to +85°C, measure only 82mm x 50mm and have an especially low-profile design thanks to the use of edge card connectors. Nevertheless, there is still enough space for up to a 64GB on-board SSD to store OS and application data. A highlight of the pin-out is the mobile feature set with 3 UARTs with complete function range also for, e.g., GPS as well as support of the MIPI-compliant serial camera interface (MIPI CSI = Mobile Industry Processor Interface Camera Serial Interface). The powerful Intel® Gen 7 Graphics are carried out via HDMI 1.4 and LVDS (optional eDP) with up to 2560x1600 and 60 Hz to the display. Further interfaces include 1x GbE LAN via Intel® Ethernet Controller I210, 1x USB 3.0 and 2x USB 2.0, amongst others. Customer-specific extensions can be implemented via 2 SDIO and 3 PCIe x1 lanes with 5GT/s.

2.2 SMARC™ Computer-on-Modules

The SMARC™ standard was developed especially for new modules with ARM- and SOC-processors and is characterized by the extremely flat build of its form factor. It is based on the MXM 3.0 connector with 314 pins and a construction height of just 4.3 millimeters and it thus allows robust and flatly constructed designs with a cost-effective card edge connector. The connector is also available in a shock- and vibration-resistant version for rough environmental conditions. Furthermore, the standard integrates dedicated interfaces for the latest ARM and SOC processors which not only means LVDS, 24-bit RGB and HDMI support but also support of embedded DisplayPort for future designs. In addition, and for the first time, dedicated camera interfaces are being incorporated into a COM standard. OEMs profit from minimized design effort and bill of material costs. SMARC™ defines two different module sizes in order to offer a high level of flexibility regarding different mechanical requirements: a short modules measuring 82 mm x 50 mm and a full-size module measuring 82 mm x 80 mm.

SMARC™ is the low-power embedded architecture platform for computer-on-modules based on ARM technology.

- » Creating mobile, embedded, connected solutions
- » Scalable building blocks
- » Optimized pin-out definition for ARM technology
- » Ultra low-power, low-profile solutions
- » Constructed to withstand harsh industrial environments

3 Product Specification

3.1 Modules & Accessories

The SMARC short sized Computer-on-Module SMARC-sXBTi (SXVV) is based on Intel's Bay Trail platform and is available in different variants to cover the demand of different performance, price and power:

Industrial temperature grade modules (E2: -40°C to +85°C operating)

Part Number	Product Name	Processor	Frequency	Memory	ECC	eMMC	Ethernet
51004-4016-19-4	SMARC-sXBTi E3845 4E/16S	BayTrail-I Intel® Atom E3845	4×1,91GHz	4GB	Yes	16GB SLC	Intel® i210IT
51004-1040-17-2	SMARC-sXBTi E3827 1E/4S	BayTrail-I Intel® Atom E3827	2×1,75GHz	1GB	Yes	4GB SLC	Intel® i210IT
51004-2000-19-4	SMARC-sXBTi E3845 2GB	BayTrail-I Intel® Atom E3845	4×1,91GHz	2GB	-	-	Intel® i210IT
51004-2000-17-2	SMARC-sXBTi E3827 2GB	BayTrail-I Intel® Atom E3827	2×1,75GHz	2GB	-	-	Intel® i210IT
51004-2000-15-2	SMARC-sXBTi E3826 2GB	BayTrail-I Intel® Atom E3826	2×1,46GHz	2GB	-	-	Intel® i210IT
51004-2000-13-2	SMARC-sXBTi E3825 2GB	BayTrail-I Intel® Atom E3825	2×1,33GHz	2GB	-	-	Intel® i210IT
51004-1000-15-1	SMARC-sXBTi E3815 1GB	BayTrail-I Intel® Atom E3815	1×1,46GHz	1GB	-	-	Intel® i210IT

Memory configurations:

- » MM = 10: 1024MB DDR3L Memory (8x1Gbit / 128Mx8)
- » MM = 20: 2048MB DDR3L Memory (8x2Gbit / 256Mx8)
- » MM = 40: 4096MB DDR3L Memory (8x4Gbit / 512Mx8)
- » MM = 80: 8192MB DDR3L Memory (8x8Gbit / 1024Mx8) (not available now, will come up in a later release)

Onboard Flash configurations

- » FF = 00: without eMMC Flash
- » FF = 20: 2GB onboard eMMC Flash
- » FF = 40: 4GB onboard eMMC Flash
- » FF = 80: 8GB onboard eMMC Flash
- » FF = 16: 16GB onboard eMMC Flash
- » FF = 32: 32GB onboard eMMC Flash
- » FF = 64: 64GB onboard eMMC Flash

Optional hardware features:

- » eDP on SMARC Connector, instead of LVDS
- » ECC memory
- » CSI 1 with 4 lanes, instead of 2x 2 lanes CSI

Optional BIOS/Software features:

- » AES-NI Support
- » FSP with Coreboot



Optional hardware and BIOS features are available project based only for variants not listed above. Please contact your local sales for customized articles.

Accessories

Product Number	Carrier Boards
51100-0000-00-S	SMARC Starterkit
Product Number	Cooling & Mounting
51004-0000-99-1	HSP SMARC-sXBT
Product Number	Adapter & Cables
59000-0000-00-0	ADA-SMARC sacrifice
59200-0000-04-0	KLAS JILI30

3.2 Functional Specification

Processor

The 32nm Intel® ATOM™ / Celeron® (BayTrail-I SOC (Valleyview)) CPU family supports:

- » Intel® 64
- » Enhanced Intel SpeedStep® Technology
- » Thermal Monitoring Technologies
- » Execute Disable Bit
- » Virtualization Technology VT-x
- » 2 Display Pipes for dual independent displays

CPU specifications

Intel®	Atom™	Atom™	Atom™	Atom™	Atom™
-	E3845	E3827	E3826	E3825	E3815
Stepping	B3/D0	B3/D0	B3/D0	B3/D0	B3/D0
# of Cores	4	2	2	2	1
# of Threads	4	2	2	2	1
CPU Nominal frequency	1.91GHz	1.75GHz	1.46GHz	1.33GHz	1.46GHz
CPU Burst frequency	-	-	-	-	-
LFM/LPM Frequency	533MHz	533MHz	533MHz	533MHz	533MHz
Tjunction	-40 to 110°C	-40 to 110°C	-40 to 110°C	-40 to 110°C	-40 to 110°C
Thermal Design Power (TDP)	10W	8W	7W	6W	5W
SDP	-	-	-	-	-
Smart Cache	2x1MB	2x512kB	2x512kB	2x512kB	512kB
Memory Type	DDR3L-1333	DDR3L-1333	DDR3L-1066	DDR3L-1066	DDR3L-1066
Max Memory Size	8GB	8GB	8GB	8GB	8GB
ECC Memory(optional)	Yes	Yes	Yes	Yes	Yes
Graphics Model	Intel HD®	Intel HD®	Intel HD®	Intel HD®	Intel HD®
GFX Base Frequency	542MHz	542MHz	533MHz	533MHz	400MHz
GFX Max Dynamic Frequ.	792MHz	792MHz	667MHz	-	-
GFX Technology	GT1 4EU	GT1 4EU	GT1 4EU	GT1 4EU	GT1 4EU
AEC Q100 automtovie Qual.	Yes	Yes	Yes	Yes	Yes
SDIO	Yes	Yes	Yes	Yes	Yes
eMMC	Yes	Yes	Yes	Yes	Yes
AES-NI (optional)	Yes	Yes	Yes	Yes	Yes

Memory

Sockets	memory down
Memory Type	DDR3L-1066/1333
Maximum Size	2 - 4GB (ECC optional)
Technology	Single Channel (64bit)

Graphics Core

The integrated Intel® HD Graphics (Gen 7) supports:

Execution Units / Pixel Pipelines	4
Max Graphics Memory	tbd
GFX Memory Bandwidth (GB/s)	tbd
GFX Memory Technology	DVMT
API (DirectX/OpenGL)	11 / 3.0 + OCL 1.1
Shader Model	3.0
Hardware accelerated Video	H.264 / MPEG1,2,4 / VC1 / WMV9 / Blu-ray
Independent/Simultaneous Displays	2
Display Port	-
HDCP support	HDCP / PAVP 2

LVDS

LVDS Bits/Pixel	1x18 / 1x24 with DP2LVDS NXP3460
LVDS Bits/Pixel with dithering	-
LVDS max Resolution:	1366x768
PWM Backlight Control:	YES
Supported Panel Data:	EDID/DID

Display Interfaces

Discrete Graphics	-
Digital Display Interface DDI1	HDMI
Digital Display Interface DDI2	-
Digital Display Interface DDI3	-
Maximum Resolution on DDI	2560x1600@60Hz

Storage

onboard SSD	2-64GB eMMC
SD Card support	Yes
IDE Interface	-
Serial-ATA	1x SATA 3Gb/s
SATA AHCI	AHCI
SATA RAID	-

Connectivity

USB 2.0	2x USB 2.0
USB 3.0	1x USB 3.0
USB Client	1 client (optional)
PCI	-
PCI External Masters	-
PCI Express	3x PCIe x1 Gen2
Max PCI Express	-
PCI Express x2/x4 configuration	-
Ethernet	10/100/1000 Mbit
Ethernet controller	Intel® i210IT / i211AT

Ethernet

The Intel® i210IT / i211AT ethernet supports:

- » Jumbo Frames
- » Time Sync Protocol Indicator
- » WOL (Wake On LAN)
- » PXE (Preboot eXecution Environment)

Misc Interfaces and Features

Audio	HD Audio and I2S
Onboard Hardware Monitor	NTC7802
Trusted Platform Module	-
Miscellaneous	3x UART / PWM FAN



SER0 and SER2 are HS-UARTs (HS=HighSpeed), SER1 is a SIO-UART and is used for console redirection. HS-UARTs and SIO-UARTs cannot be used simultaneously.

Kontron Features

External I2C Bus	5 x I2C (PM, CAM, LVDS, GP, HDMI)
M.A.R.S. support	-
Embedded API	KEAPI3 planned
Custom BIOS Settings / Flash Backup	YES
Watchdog support	Yes

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	3,0V - 5,25V
ACPI	ACPI 5.0
S-States	S0, S3, S4, S5
S5 Eco Mode	tbd
Misc Power Management	DPST 4.0, iFFS

Power Consumption and Performance

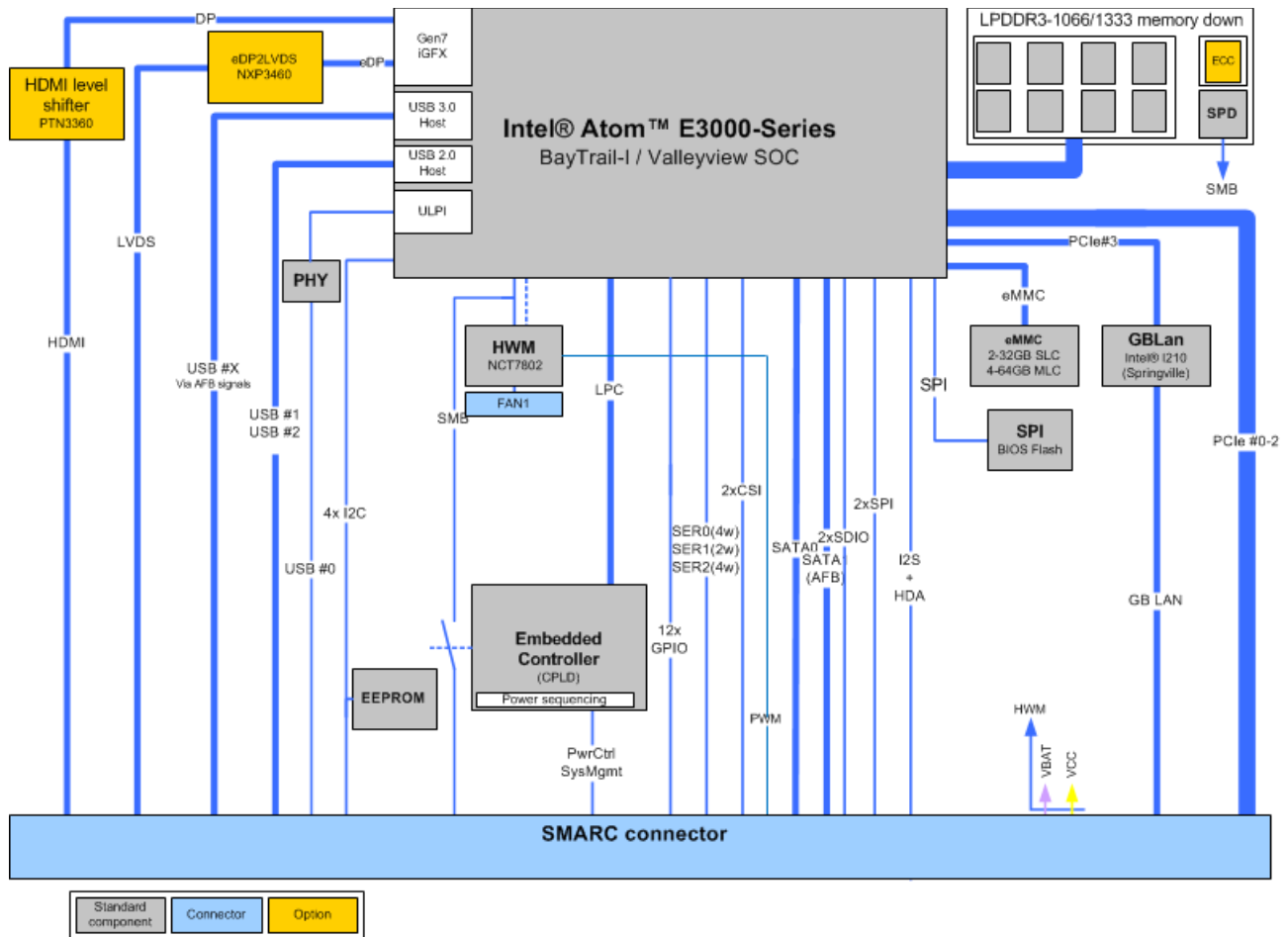
Full Load Power Consumption	tbd
Kontron Performance Index	tbd
Kontron Performance/Watt	tbd

Supported Operating Systems

The SMARC-sXBTi supports:

- » Microsoft Windows 8 32bit/64bit
- » Microsoft Windows Embedded Standard 8 (WES8)
- » Microsoft Windows 7 32bit/64bit
- » Microsoft Windows Embedded Standard 7 (WES7)
- » Microsoft Windows Embedded Compact 7 (WEC7)
- » Linux
- » WindRiver VxWorks 6.9 32bit/64bit

3.3 Block Diagram



3.4 Electrical Specification

3.4.1 Supply Voltage

Following supply voltage is specified at the SMARCTM connector:

VCC:	3,0V - 5,25V
RTC:	2,5V - 3,3V

3.4.2 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

3.4.3 Supply Voltage Ripple

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

3.5 Power Control

Power Supply

The SMARC-sXBTi supports a power input from 3,0V - 5,25V. The supply voltage is applied through the VCC pins (VCC) of the module connector.

Power Button (PWR_BTN#)

The power button (Pin P128) 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).

CB_POWER_BAD#

The SMARC-sXBTi provides an external input for a Carrier Board Power Bad signal (Pin S150). The implementation of this subsystem complies with the SMARC Specification. CB_POWER_BAD# is internally pulled up to 3.3V and must be high level to power on the module.

Reset Button (RST_CB_IN#)

The reset button (Pin P127) is available through the module connector described in the pinout list. The module will stay in reset as long as RST_CB_IN# is grounded.

3.6 Environmental Specification

3.6.1 Temperature Specification

General Specification	Operating	Non-operating
Commercial grade	0°C to +60°C	-30°C to +85°C
Extended (E1)	-25°C to +75°C	-30°C to +85°C
Industrial grade (E2)	-40°C to +85°C	-40°C to +85°C



Standard modules are available for industrial grade temperature range. Please see chapter Product Specification for available variants for extended or commercial temperate grade

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

Without Kontron heatspreader plate assembly

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

3.6.2 Humidity

- » Operating: 10% to 90% (non condensing)
- » Non operating: 5% to 95% (non condensing)

3.7 Standards and Certifications

RoHS



The **SMARC-sXBTi**

is compliant to the directive 2002/95/EC on the restriction of the use of certain hazardous substances (RoHS) in electrical and electronic equipment.

CE marking



The **SMARC-sXBTi**

is CE marked according to Low Voltage Directive 2006/95/EC – Test standard EN60950

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.

EMC

Validated in Kontron reference housing for EMC the **SMARC-sXBTi** follows the requirements for electromagnetic compatibility standards

» EN55022

3.8 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 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): 176227@40°C



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.

3.9 Mechanical Specification

3.9.1 Module Dimension

» 50mm x 82mm

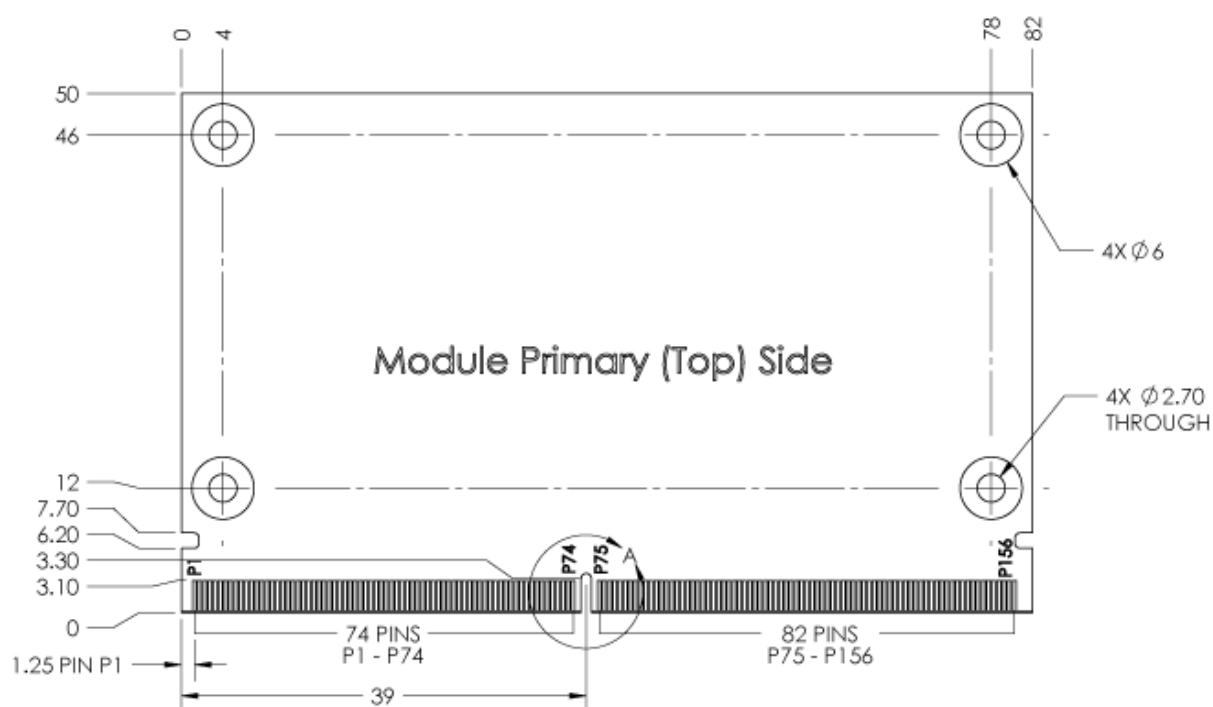
3.9.2 Height on Top

- » Maximum 3.0mm (without printed circuit board)
- » Height is depending on (optional) CPU cooler / heat spreader

3.9.3 Height on Bottom

» Maximum approx. 1.3mm (without printed circuit board)

3.9.4 Mechanical Drawing

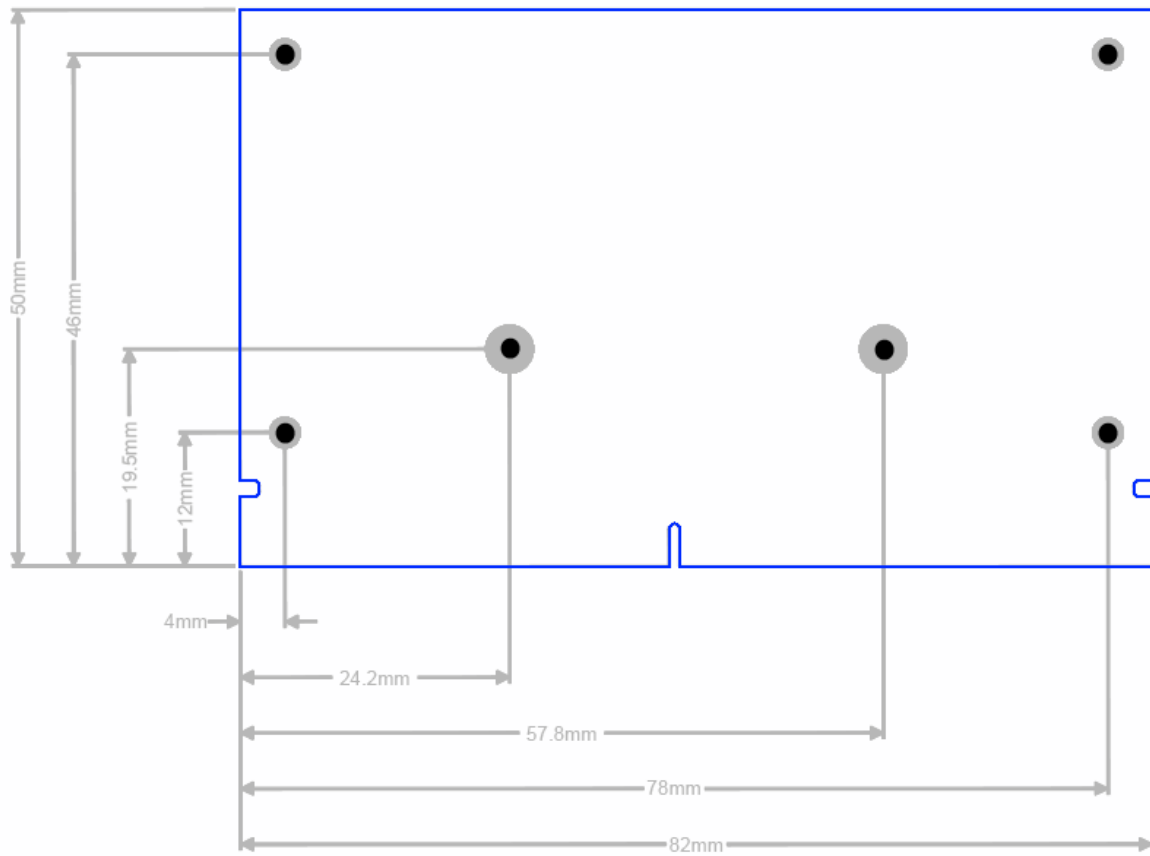


All dimensions are shown in millimeters. Tolerances should be $\pm 0.25\text{mm}$ [$\pm 0.010''$], unless otherwise noted.



CAD drawings will be available at [EMD CustomerSection](#)

3.10 Module Dimensions



All dimensions in mm

3.11 Thermal Management, Heatspreader and Cooling Solutions

A heatspreader plate assembly is available from Kontron Europe GmbH for the SMARC-sXBTi. The heatspreader plate on top of this assembly is NOT a heat sink. It works as a SMARC-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 SMARC-sXBTi. 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 SMARC application and environmental conditions. Active or passive cooling solutions provided from Kontron Europe GmbH for the SMARC-sXBTi are usually designed to cover the power and thermal dissipation for a commercial grade temperature range used in a housing with proper air flow.

4 Features and Interfaces

4.1 Onboard eMMC Flash

The SMARC-sXBTi features a 12x16mm onboard Kingston NAND Flash drive with capacities of 2-64GB eMMC. The Flash drive supports:

- » Compliant to JEDEC/eMMC standard version 4.4, 4.41 & 4.5
- » 1 bit, 4 bits or 8 bits data bus width support
- » Data transfer rate up to 52Mbyte/s using 8 parallel data lines at 52MHz
- » Single data rate up to 200Mbyte/s @ HS200 mode with 200MHz Host clock
- » Dual data rate up to 104Mbyte/s @ 52MHz
- » Error free memory access (ECC and enhanced data management)
- » TRIM support
- » Multi-Level-Cell (MLC) technology
- » Single-Level-Cell (SLC) technology
- » Industrial temperature grade -45 to +85°C

Flash Part No.	KE4CN2H5C-xxx	KE4CN3H5C-xxx	KE4CN4K6C-xxx	KE4CN5B6C-xxx	KE4CN6C6C-xxx
Nominal Flash Size MLC	4GByte	8GByte	16GByte	32GByte	64GByte
Nominal Flash Size pSLC	2GByte	4GByte	8GByte	16GByte	32GByte
JEDEC Standard	eMMC 4.5	eMMC 4.5	eMMC 4.5	eMMC 4.5	eMMC 4.5
Flash Technology	19nm	19nm	19nm	19nm	19nm
Sequential Read	85 MB/s	160 MB/s	166 MB/s	166 MB/s	166 MB/s
Sequential Write	12 MB/s	25 MB/s	25 MB/s	45 MB/s	25 MB/s
I/O Performance read/write	5000/1050 IOPS	5000/1350 IOPS	5000/1350 IOPS	4600/1450 IOPS	4600/1450 IOPS
Operating Temperature	-40 to +85°C	-40 to +85°C	-40 to +85°C	-40 to +85°C	-25 to +85°C
Package	FBGA153	FBGA153	FBGA169	FBGA169	FBGA169
Endurance (# of P/E cycles)	MLC 3k, SLC 30k	MLC 3k, SLC 30k	MLC 3k, SLC 30k	MLC 3k, SLC 30k	MLC 3k, SLC 30k



Note: the onboard eMMC Flash requires pre-configuration via EFI Shell before OS installation (e.g. diskpart utility)

4.2 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

4.3 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.

4.4 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.

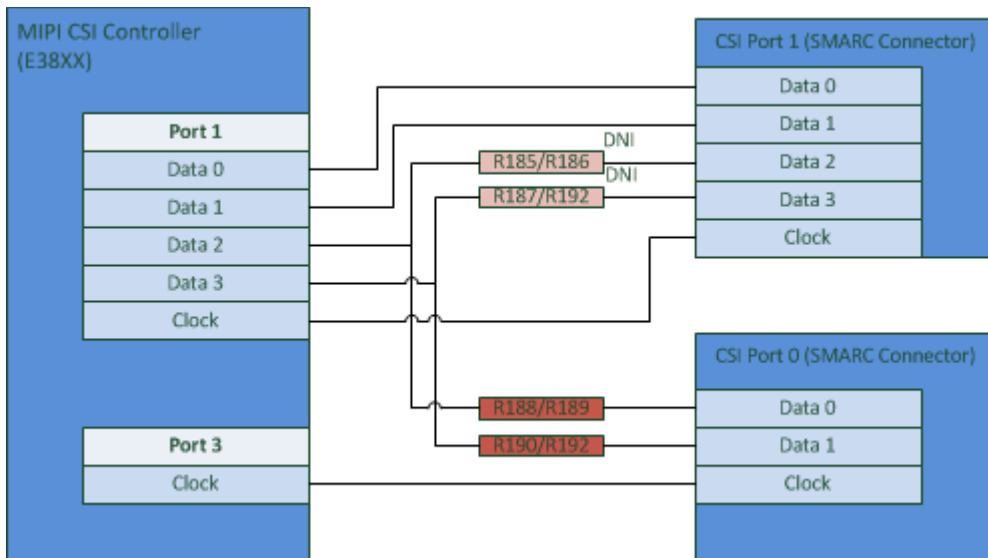
» Active C6-State may influence data transfer on external Serial Ports

» 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.

4.5 Camera Interfaces

The SMARC-sXBTi supports up to two MIPI CSI Ports defined in SMARC specification. The standard configuration supports 2 CSI Ports each with 2 lanes. Via resistor configuration CSI port 1 can be used with 4 lanes, but then CSI port 0 cannot be used anymore.



4.6 Graphics Features

The integrated Intel® HD Graphics (Gen 7) graphics supports following OS dependent featureset:

O/S	Win8 / WES8	Win7 / WES7	WEC7	Linux (F18/Yocto1.6)	Linux (Tizen IVI 32b)	Android 4.2/4.4
DisplayPort	DP 1.1a up to 2560×1600					not supported
HDMI (via external LS)	HDMI 1.4a up to 1920×1200					
VGA (COMe-compact only)	up to 2560×1600					not supported
eDP	eDP 1.3 up to 2560×1600 or LVDS up to 1920×1080 via eDP-LVDS Bridge					
Dual Independent Display	Yes					
2D HW acceleration	DirectDraw			X Server	Wayland Compositor	OpenGL Renderer
3D HW acceleration	OGL4.0, DX11.1/10/9		OGLES 2.0	OGL3.2/OGLES2.0		OGLES 1.1/2.0 in 4.2 OGLES 1.1/2.0/3.0 in 4.4 KitKat
HW Media Acceleration	DXVA 2		DirectShow	VAAPI	OGL3.2/OGLES2.0	OpenMax
HW Video Decode	H.264,MPEG2,VC1,VP8		H.264,MPEG2,VC1	H.264,MPEG2,VC1,VP8	H.264,MPEG2,VC1,VP8	H.264,H.263,VC1,WMV 9,VP8,MPEG4 in 4.2 H.264, VC1 in 4.4
HW Video Encode	H.264,MPEG2		not supported	H.264,MPEG2	H.264,MPEG2	H.264
Blu-Ray	v2.0					not supported
Media players	Windows Media Player PowerDVD		CEPlayer	GStreamer - VAAPI		Gallery, Widevine
Content Protection*	PAVP	HDCP	not supported			Widevine L1

* Supported with active TXE Engine only (available with custom BIOS only)

4.7 ACPI Suspend Modes and Resume Events

The SMARC-sXBTi supports the S-states S0, S3, S4, S5. S5eco Support: tbd

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
0	Timer0
1	Keyboard
2	Redirected secondary PIC
3	Onboard - COM2
4	Onboard - COM1
5	SIO COM3 or 4
6	SIO COM3 or 4
7	SIO LPT or COM3/4
8	RTC
9	Free for PCI devices
10	Free for PCI devices
11	Free for PCI devices
12	PS/2 mouse or free for PCI devices
13	FPU
14	not used
15	not used

5.2 Memory Area

Address range (hex)	Size	Usage
00000000-0009FFFF	640 KB	DOS- (Real mode-) memory
000A0000-000BFFFF	128 KB	Display memory
000C0000-000CBFFF	48 KB	VGA BIOS
000CC000-000DFFFF	80 KB	Option ROM or XMS
000E0000-000EFFFF	64 KB	System BIOS extended space
000F0000-000FFFFF	64 KB	System BIOS base segment
0x20000000-00100000-7FFFFFFF	2 GB – 1 MB	System memory (Low DRAM)
0x20000000-0x20001000	4KB	Minimum mapping for chipset LPE device
80000000-FFF00000	2 GB – 1 MB	PCI memory, other extensions (Low MMIO)
FEC00000-FEC00040	64 Bytes	IOxAPIC
FED00000-FED003FF	1 KB	HPET (Timer)
FED1C000-FED1CFFF	4KB	Chipset internal register space
FED40000-FED4B000	44 KB	TPM hard coded memory
FFFF0000-FFFFFFFF	64 KB	Mapping space for BIOS ROM/Boot vector
100000000-17FFFFFFF	2 GB	System memory (High DRAM)
180000000-F00000000	58 GB	High MMIO

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	Usage
0000-000F	DMA-Controller Master (8237)
0020-0021 024-025 028-029 02C-02D 030-031 034-035 038-039 03C-03D	Interrupt-Controller Master (8259)
002E-002F	External SuperI/O
040-043 050-053	Programmable Interrupt Timer (8253)
04E-04F	TPM
060, 064	KBD Interface-Controller (8042)
061, 063, 065, 067	NMI Controller
070-071	RTC CMOS / NMI mask
072-073	RTC Extended CMOS
080-083	Debug port
0A0-0A1 0A4-0A5 0A8-0A9 0AC-0AD 0B0-0B1 0B4-0B5 0B8-0B9 0BC-0BD	Interrupt-Controller Slave (8259)
0B2-0B3	APM control
279	ISA PnP
295-296	External Hardware monitor, optionally used by external SuperIO if present
2E8-2EF	Serial port COM4 (SIO COM2)
2F8-2FF	Serial port COM2 (onboard COM2)
370-377	Floppy disk controller, optionally used by external SuperIO if present (370h to 371h)
378-37F	Parallel port LPT 1, optionally used by external SuperIO if present
3C0-3CF	VGA/EGA
3E8-3EF	Serial port COM3 (SIO COM1)
3F8-3FF	Serial Port COM1 (onboard COM1)
400-4FF	Chipset internal register I/O area
4D0-4D1	Interrupt-Controller (Slave)
500-5FF	Chipset internal register I/O area
A80-A81	Kontron CPLD control port
CF8	PCI configuration address
CF9	Reset control
CFC-CFF	PCI configuration data

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.

Device	Bus/Device/Function	VID/DID default	Comment
Transaction Router (former host bridge)	0/0/0	8086h/0F00h	-
Graphics & display	0/2/0	8086h/0F31h	-
Camera image signal processor	0/3/0	8086h/0F38h	Not used
eMMC	0/16/0	8086h/0F14h	-
SDIO	0/17/0	8086h/0F15h	Not used
SD	0/18/0	8086h/0F16h	-
SATA	0/19/0	8086h/0F23h	-
xHCI	0/20/0	8086h/8C31h	-
Low-power Audio	0/21/0	8086h/0F28h	-
I2S port 0	0/21/1	-	-
I2S port 1	0/21/2	-	-
I2S port 2	0/21/3	-	-
USB3.0 device	0/22/0	8086h	-
SIO I2C DMA Configuration	0/24/0	8086h/0F40h	-
I2C1 Configuration	0/24/1	8086h/0F41h	-
I2C2 Configuration	0/24/2	8086h/0F42h	-
I2C3 Configuration	0/24/3	8086h/0F43h	-
I2C4 Configuration	0/24/4	8086h/0F44h	-
I2C5 Configuration	0/24/5	8086h/0F45h	-
I2C6 Configuration	0/24/6	8086h/0F46h	-
I2C7 Configuration	0/24/7	8086h/0F47h	-
Trusted Execution engine	0/26/0	8086h/0F18h	-
HD Audio	0/27/0	8086h/0F04h	-
PCIExpress Root port 0	0/28/0	8086h	-
PCIExpress Root port 1	0/28/1	-	-
PCIExpress Root port 2	0/28/2	-	-
PCIExpress Root port 3	0/28/3	-	-
EHCI	0/29/0	8086h/0F34h	-
SerialIO HSUART / PWM / SPI DMA	0/30/0	8086h/0F06h	-
PWM Port 1	0/30/1	8086h	-
PWM Port 2	0/30/2	8086h	-
HSUART1	0/30/3	8086h/0F0Ah	-
HSUART2	0/30/4	8086h/0F0Ch	-
SPI	0/30/5	8086h/0F0Eh	-
PCU LPC	0/31/0	8086h/0F1Ch	-

5.5 LPC addresses

I/O address	Device
4Eh/4Fh	TPM
0A80h/0A81h	CPLD

5.6 I2C Bus

8-bit Address	7-bit Address	Device	Bus
58h	0x2C	S5eco resistor	internal
5Ah	0x2D	USB HSIC Hub	internal
80h	0x40	DP2LVDS bridge	internal
A0h	0x50	LVDS EEPROM	internal
A0h	0x50	Module / JIDA EEPROM	external
Aeh	0x57	Carrier EEPROM	external

5.7 System Management (SM) Bus

8-bit Address	7-bit Address	Device	Bus
30h	0x18	DDR3L 0 Thermal sensor option	internal
5Ah	0x2D	onboard HWMonitor	internal
A0h	0x50	DDR3L SPD 0	internal
C8h	0x64	Ethernet	internal
12h	0x09	SMART_CHARGER	external
14h	0x0A	SMART_SELECTOR	external
16h	0x0B	SMART_BATTERY	external



Do not use any reserved addresses mentioned above for other devices

6 Connectors

The pinouts for Interface Connector are documented for convenient reference. Please see the SMARC Specification and SMARC Design Guide for detailed, design-level information.

6.1 SMARC™ Connector Top Side

Pin	Signal	Module Direction	Module Termination	Type/Tolerance	Controller	Controller Pin Name	Power Rail
P1	PCAM_PXL_CK1	NC	-	-	-	-	-
P2	GND	-	-	-	-	-	-
P3	CSI1_CK+ / PCAM_D0	In	-	LVDS D-PHY / VDD_IO	ValleyView	MCSI1_CLKP	V_1V24_S0
P4	CSI1_CK- / PCAM_D1	In	-	LVDS D-PHY / VDD_IO	ValleyView	MCSI1_CLKN	V_1V24_S0
P5	PCAM_DE	-	-	-	-	-	-
P6	PCAM_MCK	-	-	-	-	-	-
P7	CSI1_D0+ / PCAM_D2	In	-	LVDS D-PHY / VDD_IO	ValleyView	MCSI1_DP0	V_1V24_S0
P8	CSI1_D0- / PCAM_D3	In	-	LVDS D-PHY / VDD_IO	ValleyView	MCSI1_DN0	V_1V24_S0
P9	GND	-	-	-	-	-	-
P10	CSI1_D1+ / PCAM_D4	In	-	LVDS D-PHY / VDD_IO	ValleyView	MCSI1_DP1	V_1V24_S0
P11	CSI1_D1- / PCAM_D5	In	-	LVDS D-PHY / VDD_IO	ValleyView	MCSI1_DN1	V_1V24_S0
P12	GND	-	-	-	-	-	-
P13	CSI1_D2+ / PCAM_D6	In	-	LVDS D-PHY / VDD_IO	ValleyView	MCSI1_DP2	V_1V24_S0
P14	CSI1_D2- / PCAM_D7	In	-	LVDS D-PHY / VDD_IO	ValleyView	MCSI1_DN2	V_1V24_S0
P15	GND	-	-	-	-	-	-
P16	CSI1_D3+ / PCAM_D8	IN	-	LVDS D-PHY / VDD_IO	ValleyView	MCSI1_DP3	V_1V24_S0
P17	CSI1_D3- / PCAM_D9	IN	-	LVDS D-PHY / VDD_IO	ValleyView	MCSI1_DN3	V_1V24_S0
P18	GND	-	-	-	-	-	-
P19	GBE_MDI3-	Bi-Dir	-	GBE MDI	Springville i210	MDI3-	-
P20	GBE_MDI3+	Bi-Dir	-	GBE MDI	Springville i210	MDI3+	-
P21	GBE_LINK100#	Out / OD	-	VDD_IO	Springville i210	LED1	V_3V3_GBE
P22	GBE_LINK1000#	Out / OD	-	VDD_IO	Springville i210	LED2	V_3V3_GBE
P23	GBE_MDI2-	Bi-Dir	-	GBE MDI	Springville i210	MDI2-	-
P24	GBE_MDI2+	Bi-Dir	-	GBE MDI	Springville i210	MDI2+	-
P25	GBE_LINK_ACT#	Out / OD	-	VDD_IO	Springville i210	LED0	V_3V3_GBE
P26	GBE_MDI1-	Bi-Dir	-	GBE MDI	Springville i210	MDI1-	-
P27	GBE_MDI1+	Bi-Dir	-	GBE MDI	Springville i210	MDI1+	-
P28	GBE_CTREF	-	-	-	-	-	-
P29	GBE_MDI0-	Bi-Dir	-	GBE MDI	Springville i210	MDI0-	-
P30	GBE_MDI0+	Bi-Dir	-	GBE MDI	Springville i210	MDI0+	-
P31	SPIO_CS1#	-	PU-100k	CMOS / VDD_IO	-	-	V_1V8_S0
P32	GND	-	-	-	-	-	-
P33	SDIO_WP	In	-	CMOS 3.3V	ValleyView	SD3_WP	V_1V8_S0
P34	SDIO_CMD	Bi-Dir	Series-220hm + PU-20k	CMOS 3.3V	ValleyView	SD3_CMD	V_3V3_S0
P35	SDIO_CD#	In	-	CMOS 3.3V	ValleyView	SD3_CD#	V_1V8_S0
P36	SDIO_CK	Out	Series-220hm + PD-20k	CMOS 3.3V	ValleyView	SD3_CLK	V_3V3_S0
P37	SDIO_PWR_EN	Out	-	CMOS 3.3V	ValleyView	SD3_PWREN#	V_1V8_S0
P38	GND	-	-	-	-	-	-
P39	SDIO_D0	Bi-Dir	PU-20k	CMOS 3.3V	ValleyView	SD3_D0	V_3V3_S0
P40	SDIO_D1	Bi-Dir	PU-20k	CMOS 3.3V	ValleyView	SD3_D1	V_3V3_S0
P41	SDIO_D2	Bi-Dir	PU-20k	CMOS 3.3V	ValleyView	SD3_D2	V_3V3_S0
P42	SDIO_D3	Bi-Dir	PU-20k	CMOS 3.3V	ValleyView	SD3_D3	V_3V3_S0
P43	SPIO_CS0#	Out	Series-220hm	CMOS / 1.8V	ValleyView	PCU_SPI_CS1#	V_VIO_S0
P44	SPIO_CK	Out	Series-220hm	CMOS / 1.8V	ValleyView	PCU_SPI_CLK	V_VIO_S0
P45	SPIO_DIN	In	Series-220hm	CMOS / 1.8V	ValleyView	PCU_SPI_MISO	V_VIO_S0
P46	SPIO_D0	Out	Series-220hm	CMOS / 1.8V	ValleyView	PCU_SPI_MOSI	V_VIO_S0
P47	GND	-	-	-	-	-	-
P48	SATA_TX+	Out	Serial 10nF	SATA	ValleyView	SATA_TXP0	-
P49	SATA_TX-	Out	Serial 10nF	SATA	ValleyView	SATA_TXN0	-

P50	GND	-	-	-	-	-	-
P51	SATA_RX+	In	Serial 10nF	SATA	ValleyView	SATA_RXP0	-
P52	SATA_RX-	In	Serial 10nF	SATA	ValleyView	SATA_RXN0	-
P53	GND	-	-	-	-	-	-
P54	SPI1_CS0#	Out	Series-33.20hm	CMOS / 1.8V	ValleyView	SIO_SPI_CS#	V_1V8_S0
P55	SPI1_CS1#	-	PU-100k	CMOS / VDD_IO	-	-	V_1V8_S0
P56	SPI1_CK	Out	Series-33.20hm	CMOS / 1.8V	ValleyView	SIO_SPI_CLK	V_1V8_S0
P57	SPI1_DIN	In	-	CMOS / 1.8V	ValleyView	SIO_SPI_MISO	V_1V8_S0
P58	SPI1_DO	Out	Series-33.20hm	CMOS / 1.8V	ValleyView	SIO_SPI_MOSI	V_1V8_S0
P59	GND	-	-	-	-	-	-
P60	USB0+	Bi-Dir	-	USB	TUSB1211A1ZRQ	DP	-
P61	USB0-	Bi-Dir	-	USB	TUSB1211A1ZRQ	DM	-
P62	USB0_EN_OC#	Bi-Dir / OD	PU-CPLD-5-25k	CMOS 3.3V	TUSB1211+CPLD	FAULT/PSW	V_1V8_S5
P63	USB0_VBUS_DET	In	-	CMOS 5.0V	TUSB1211A1ZRQ	VBUS	V_1V8_S5
P64	USB0_OTG_ID	In	-	CMOS 3.3V	TUSB1211A1ZRQ	ID	V_1V8_S5
P65	USB1+	Bi-Dir	-	USB	ValleyView	USB_DP2	-
P66	USB1-	Bi-Dir	-	USB	ValleyView	USB_DN2	-
P67	USB1_EN_OC#	Bi-Dir	PU-CPLD-10k	CMOS 3.3V	CPLD	IO_H2	V_3V3_REG_S5
P68	GND	-	-	-	-	-	-
P69	USB2+	Bi-Dir	-	USB	ValleyView	USB_DP3	-
P70	USB2-	Bi-Dir	-	USB	ValleyView	USB_DN3	-
P71	USB2_EN_OC#	Bi-Dir	PU-CPLD-10k	CMOS 3.3V	CPLD	IO_D3	V_3V3_REG_S5
P72	PCIE_C_PRST#	In	PU-10k	CMOS 3.3V	ValleyView	ILB_LPC_SERIRQ	V_1V8_S0
P73	PCIE_B_PRST#	In	PU-10k	CMOS 3.3V	ValleyView	ILB_LPC_CLK0	V_1V8_S0
P74	PCIE_A_PRST#	In	PU-10k	CMOS 3.3V	ValleyView	ILB_LPC_AD3	V_1V8_S0
-	<Key>	-	-	-	-	-	-
P75	PCIE_A_RST#	Out	-	CMOS 3.3V	ValleyView	PMC_PLTRST#	V_1V8_S0
P76	PCIE_C_CLKREQ#	In	PU-10k	CMOS 3.3V	ValleyView	PCIE_CLKREQ2#	V_1V8_S0
P77	PCIE_B_CLKREQ#	In	PU-10k	CMOS 3.3V	ValleyView	PCIE_CLKREQ1#	V_1V8_S0
P78	PCIE_A_CLKREQ#	In	PU-10k	CMOS 3.3V	ValleyView	PCIE_CLKREQ0#	V_1V8_S0
P79	GND	-	-	-	-	-	-
P80	PCIE_C_REFCK+	Out	-	LVDS PCIe	ValleyView	PCIE_CLKP2	-
P81	PCIE_C_REFCK-	Out	-	LVDS PCIe	ValleyView	PCIE_CLKN2	-
P82	GND	-	-	-	-	-	-
P83	PCIE_A_REFCK+	Out	-	LVDS PCIe	ValleyView	PCIE_CLKP0	-
P84	PCIE_A_REFCK-	Out	-	LVDS PCIe	ValleyView	PCIE_CLKN0	-
P85	GND	-	-	-	-	-	-
P86	PCIE_A_RX+	In	-	LVDS PCIe	ValleyView	PCIE_RXP0	-
P87	PCIE_A_RX-	In	-	LVDS PCIe	ValleyView	PCIE_RXN0	-
P88	GND	-	-	-	-	-	-
P89	PCIE_A_TX+	Out	Serial-100nF	LVDS PCIe	ValleyView	PCIE_TXP0	-
P90	PCIE_A_TX-	Out	Serial-100nF	LVDS PCIe	ValleyView	PCIE_TXN0	-
P91	GND	-	-	-	-	-	-
P92	HDMI_D2+	Out	-	TMDS	PTN3360B Shifter	OUT_D4+	-
P93	HDMI_D2-	Out	-	TMDS	PTN3360B Shifter	OUT_D4-	-
P94	GND	-	-	-	-	-	-
P95	HDMI_D1+	Out	-	TMDS	PTN3360B Shifter	OUT_D3+	-
P96	HDMI_D1-	Out	-	TMDS	PTN3360B Shifter	OUT_D3-	-
P97	GND	-	-	-	-	-	-
P98	HDMI_D0+	Out	-	TMDS	PTN3360B Shifter	OUT_D2+	-
P99	HDMI_D0-	Out	-	TMDS	PTN3360B Shifter	OUT_D2-	-
P100	GND	-	-	-	-	-	-
P101	HDMI_CK+	Out	-	TMDS	PTN3360B Shifter	OUT_D1+	-
P102	HDMI_CK-	Out	-	TMDS	PTN3360B Shifter	OUT_D1-	-
P103	GND	-	-	-	-	-	-
P104	HDMI_HPD	In	PU-100k	CMOS 1.8V	PTN3360B Shifter	HPD_SINK	V_1V8_S0
P105	HDMI_CTRL_CK	Out	PU-100k	CMOS 1.8V	PTN3360B Shifter	SCL_SINK	V_1V8_S0
P106	HDMI_CTRL_DAT	Bi-Dir	PU-100k	CMOS 1.8V	PTN3360B Shifter	SDA_SINK	V_1V8_S0
P107	HDMI_CEC	-	-	-	-	-	-
P108	GPIO0 / CAM0_PWR#	Bi-Dir	PU-SoC-20k	CMOS / 1.8V	ValleyView	GPIO_S0_SC_88	V_1V8_S0
P109	GPIO1 / CAM1_PWR#	Bi-Dir	PU-SoC-20k	CMOS / 1.8V	ValleyView	GPIO_S0_SC_89	V_1V8_S0
P110	GPIO2 / CAM0_RST#	Bi-Dir	PU-SoC-20k	CMOS / 1.8V	ValleyView	GPIO_S0_SC_91	V_1V8_S0
P111	GPIO3 / CAM1_RST#	Bi-Dir	PU-SoC-20k	CMOS / 1.8V	ValleyView	GPIO_S0_SC_90	V_1V8_S0
P112	GPIO4 / HDA_RST#	Bi-Dir	PU-SoC-20k	CMOS / 1.8V	ValleyView	GPIO_S0_SC_59	V_1V8_S0
P113	GPIO5 / PWM_OUT	Bi-Dir	PU-SoC-20k	CMOS / 1.8V	ValleyView	GPIO_S0_SC_93	V_1V8_S0

P114	GPIO6 / TACHIN	Bi-Dir	PU-SoC-20k	CMOS / 1.8V	ValleyView	GPIO_S0_SC_92	V_1V8_S0
P115	GPIO7 / PCAM_FLD	Bi-Dir	PU-SoC-20k	CMOS / 1.8V	ValleyView	GPIO_S0_SC_97	V_1V8_S0
P116	GPIO8 / CAN0_ERR #	Bi-Dir	PU-SoC-20k	CMOS / 1.8V	ValleyView	GPIO_S0_SC_98	V_1V8_S0
P117	GPIO9 / CAN1_ERR #	Bi-Dir	PU-SoC-20k	CMOS / 1.8V	ValleyView	GPIO_S0_SC_99	V_1V8_S0
P118	GPIO10	Bi-Dir	PU-SoC-20k	CMOS / 1.8V	ValleyView	GPIO_S0_SC_100	V_1V8_S0
P119	GPIO11	Bi-Dir	PU-SoC-20k	CMOS / 1.8V	ValleyView	GPIO_S0_SC_101	V_1V8_S0
P120	GND	-	-	-	-	-	-
P121	I2C_PM_CK	Out	PU-2k2	CMOS 1.8V	ValleyView	SIO_I2C_DATA / _G PIO_S0_SC_79	V_1V8_S0
P122	I2C_PM_DAT	Bi-Dir	PU-2k2	CMOS 1.8V	ValleyView	SIO_I2C_DATA / _G PIO_S0_SC_79	V_1V8_S0
P123	BOOT_SEL0#	In	PU-SoC-20k	CMOS / 1.8V	ValleyView	GPIO_S5_0	V_1V8_S5
P124	BOOT_SEL1#	In	PU-SoC-20k	CMOS / 1.8V	ValleyView	GPIO_S5_8	V_1V8_S5
P125	BOOT_SEL2#	In	PU-SoC-20k	CMOS / 1.8V	ValleyView	GPIO_S5_10	V_1V8_S5
P126	RESET_OUT#	Out	CPLD-Wpu	CMOS / 1.8V	CPLD	IO_B5	V_1V8_REG_S5
P127	RESET_IN#	In	PU-CPLD-20k	CMOS / 1.8V	CPLD	IO_J10	V_1V8_REG_S5
P128	POWER_BTN#	In	PU-CPLD-20k	CMOS / 1.8V	CPLD	IO_E10	V_1V8_REG_S5
P129	SER0_TX	Out	SoC 20k PU	CMOS / VDD_IO	ValleyView	SIO_UART1_TXD	V_1V8_S0
P130	SER0_RX	In	SoC 20k PU	CMOS / VDD_IO	ValleyView	SIO_UART1_RXD	V_1V8_S0
P131	SER0_RTS#	Out	SoC 20k PU	CMOS / VDD_IO	ValleyView	SIO_UART1_RTS#	V_1V8_S0
P132	SER0_CTS#	In	SoC 20k PU	CMOS / VDD_IO	ValleyView	SIO_UART1_CTS#	V_1V8_S0
P133	GND	-	-	-	-	-	-
P134	SER1_TX	Out	SoC 20k PU	CMOS / VDD_IO	ValleyView	GPIO_S0_SC_57	V_1V8_S0
P135	SER1_RX	In	SoC 20k PU	CMOS / VDD_IO	ValleyView	GPIO_S0_SC_61	V_1V8_S0
P136	SER2_TX	Out	SoC 20k PU	CMOS / VDD_IO	ValleyView	SIO_UART2_TXD	V_1V8_S0
P137	SER2_RX	In	SoC 20k PU	CMOS / VDD_IO	ValleyView	SIO_UART2_RXD	V_1V8_S0
P138	SER2_RTS#	Out	SoC 20k PU	CMOS / VDD_IO	ValleyView	SIO_UART2_RTS#	V_1V8_S0
P139	SER2_CTS#	In	SoC 20k PU	CMOS / VDD_IO	ValleyView	SIO_UART2_CTS#	V_1V8_S0
P140	SER3_TX	NC	-	-	-	-	-
P141	SER3_RX	NC	-	-	-	-	-
P142	GND	-	-	-	-	-	-
P143	CAN0_TX	NC	-	-	-	-	-
P144	CAN0_RX	NC	-	-	-	-	-
P145	CAN1_TX	NC	-	-	-	-	-
P146	CAN1_RX	NC	-	-	-	-	-
P147	VDD_IN	PWR	-	-	-	-	3.0V-5.25V
P148	VDD_IN	PWR	-	-	-	-	3.0V-5.25V
P149	VDD_IN	PWR	-	-	-	-	3.0V-5.25V
P150	VDD_IN	PWR	-	-	-	-	3.0V-5.25V
P151	VDD_IN	PWR	-	-	-	-	3.0V-5.25V
P152	VDD_IN	PWR	-	-	-	-	3.0V-5.25V
P153	VDD_IN	PWR	-	-	-	-	3.0V-5.25V
P154	VDD_IN	PWR	-	-	-	-	3.0V-5.25V
P155	VDD_IN	PWR	-	-	-	-	3.0V-5.25V
P156	VDD_IN	PWR	-	-	-	-	3.0V-5.25V

6.2 SMARC™ Connector Bottom Side

Pin	Signal	Module Direction	Module Termination	Type/Tolerance	Controller	Controller Pin Name	Power Rail
S1	PCAM_VSYNC	-	-	-	-	-	-
S2	PCAM_HSYNC	-	-	-	-	-	-
S3	GND	-	-	-	-	-	-
S4	PCAM_PXL_CK0	-	-	-	-	-	-
S5	I2C_CAM_CK	Out	PU-2k2	CMOS / 1.8V	ValleyView	STIO_I2C1_CLK/_G PIO_S0_SC_80	V_1V8_S0
S6	CAM_MCK	Out	-	CMOS / 1.8V	ValleyView	PMC_PLT_CLK0	V_1V8_S0
S7	I2C_CAM_DAT	Bi-Dir	PU-2k2	CMOS / 1.8V	ValleyView	STIO_I2C1_DATA/_ GPIO_S0_SC_81	V_1V8_S0
S8	CSIO_CK+ / PCAM_D10	In	-	LVDS D-PHY / 1.8V	ValleyView	MCSI3_CLKP	V_1V24_S0
S9	CSIO_CK- / PCAM_D11	In	-	LVDS D-PHY / 1.8V	ValleyView	MCSI3_CLKN	V_1V24_S0
S10	GND	-	-	-	-	-	-
S11	CSIO_D0+ / PCAM_D12	In	-	LVDS D-PHY / 1.8V	ValleyView	MCSI1_DP2	V_1V24_S0
S12	CSIO_D0- / PCAM_D13	In	-	LVDS D-PHY / 1.8V	ValleyView	MCSI1_DN2	V_1V24_S0
S13	GND	-	-	-	-	-	-
S14	CSIO_D1+ / PCAM_D14	In	-	LVDS D-PHY / 1.8V	ValleyView	MCSI1_DP3	V_1V24_S0
S15	CSIO_D1- / PCAM_D15	In	-	LVDS D-PHY / 1.8V	ValleyView	MCSI1_DN3	V_1V24_S0
S16	GND	-	-	-	-	-	-
S17	AFB0_OUT	Out	-	CMOS / 1.8V	ValleyView	PMC_SLP_S3#	V_1V8_S5
S18	AFB1_OUT	Out	-	CMOS / 1.8V	ValleyView	PMC_SLP_S4#	V_1V8_S5
S19	AFB2_OUT	Out	-	CMOS / 1.8V	ValleyView	PMC_SUS_STAT#	V_1V8_S5
S20	AFB3_IN	-	-	-	-	-	-
S21	AFB4_IN	-	-	-	-	-	-
S22	AFB5_IN	-	-	-	-	-	-
S23	AFB6_PTIO	Bi-Dir	Serial-100nF (parallel) 2000hm	CMOS / 3.3V protected	CPLD	IO_K8/DEV_CLR#	V_3V3_REG_S5
S24	AFB7_PTIO	Bi-Dir	Serial-100nF (parallel) 2000hm	CMOS / 1.8V protected	ValleyView	PCU_SMB_ALERT#	V_1V8_S0
S25	GND	-	-	-	-	-	-
S26	SDMMC_D0	Bi-Dir	PU-SoC-20k	CMOS / 1.8V	ValleyView	SD2_D0	V_1V8_S0
S27	SDMMC_D1	Bi-Dir	PU-SoC-20k	CMOS / 1.8V	ValleyView	SD2_D1	V_1V8_S0
S28	SDMMC_D2	Bi-Dir	PU-SoC-20k	CMOS / 1.8V	ValleyView	SD2_D2	V_1V8_S0
S29	SDMMC_D3	Bi-Dir	PU-SoC-20k	CMOS / 1.8V	ValleyView	SD2_D3_CD#	V_1V8_S0
S30	SDMMC_D4	-	-	-	-	-	-
S31	SDMMC_D5	-	-	-	-	-	-
S32	SDMMC_D6	-	-	-	-	-	-
S33	SDMMC_D7	-	-	-	-	-	-
S34	GND	-	-	-	-	-	-
S35	SDMMC_CK	Out	Serial-220hm + PD- SoC-20k	CMOS / 1.8V	ValleyView	SD2_CLK	V_1V8_S0
S36	SDMMC_CMD	Bi-Dir	Serial-220hm + PU- SoC-20k	CMOS / 1.8V	ValleyView	SD2_CMD	V_1V8_S0
S37	SDMMC_RST#	Out	-	CMOS / 1.8V	ValleyView	PMC_PLTRST#	V_1V8_S5
S38	AUDIO_MCK	-	-	-	-	-	-
S39	I2S0_LRCK	Bi-Dir	-	CMOS / 1.8V	ValleyView	LPE_I2S2_FRM	V_1V8_S0
S40	I2S0_SDOUT	Out	-	CMOS / 1.8V	ValleyView	LPE_I2S2_DATAOUT	V_1V8_S0
S41	I2S0_SDIN	In	-	CMOS / 1.8V	ValleyView	LPE_I2S2_DATAIN	V_1V8_S0
S42	I2S0_CK	Bi-Dir	-	CMOS / 1.8V	ValleyView	LPE_I2S2_CLK	V_1V8_S0
S43	I2S1_LRCK	-	-	-	-	-	-
S44	I2S1_SDOUT	-	-	-	-	-	-
S45	I2S1_SDDIN	-	-	-	-	-	-
S46	I2S1_CK	-	-	-	-	-	-
S47	GND	-	-	-	-	-	-
S48	I2C_GP_CK	Out	PU-2k2	CMOS / 1.8V	ValleyView	STIO_I2C3_CLK/_G PIO_S0_SC_84	V_1V8_S0
S49	I2C_GP_DAT	Bi-Dir	PU-2k2	CMOS / 1.8V	ValleyView	STIO_I2C3_DATA/_ GPIO_S0_SC_85	V_1V8_S0
S50	I2S2_LRCK	Bi-Dir	-	CMOS / 1.5V	ValleyView	HDA_SYNC	V_1V5_S0
S51	I2S2_SDOUT	Out	-	CMOS / 1.5V	ValleyView	HDA_SDO	V_1V5_S0
S52	I2S2_SDIN	In	Serial-220hm	CMOS / 1.5V	ValleyView	HDA_SDIO	V_1V5_S0
S53	I2S2_CK	Bi-Dir	-	CMOS / 1.5V	ValleyView	HDA_CLK	V_1V5_S0

S54	SATA_ACT#	Out-OD	-	CMOS / 3.3V	ValleyView	SATA_LED#	V_1V8_S0
S55	AFB8_PTIO	-	-	-	-	-	-
S56	AFB9_PTIO	-	-	-	-	-	-
S57	PCAM_ON_CSI0#	-	-	-	-	-	-
S58	PCAM_ON_CSI1#	-	-	-	-	-	-
S59	SPDIF_OUT	-	-	-	-	-	-
S60	SPDIF_IN	-	-	-	-	-	-
S61	GND	-	-	-	-	-	-
S62	AFB_DIFF0+	In	-	USB3.0	ValleyView	USB3_RXP0	V_1V0_S0
S63	AFB_DIFF0-	In	-	USB3.0	ValleyView	USB3_RXN0	V_1V0_S0
S64	GND	-	-	-	-	-	-
S65	AFB_DIFF1+	Out	-	USB3.0	ValleyView	USB3_TXP0	V_1V0_S0
S66	AFB_DIFF1-	Out	-	USB3.0	ValleyView	USB3_TXN0	V_1V0_S0
S67	GND	-	-	-	-	-	-
S68	AFB_DIFF2+	Bi-Dir	-	USB2.0	ValleyView	USB_DP0	-
S69	AFB_DIFF2-	Bi-Dir	-	USB2.0	ValleyView	USB_DN0	-
S70	GND	-	-	-	-	-	-
S71	AFB_DIFF3+	In	Serial-10nF	SATA	ValleyView	SATA_TXP1	-
S72	AFB_DIFF3-	In	Serial-10nF	SATA	ValleyView	SATA_TXN1	-
S73	GND	-	-	-	-	-	-
S74	AFB_DIFF4+	Out	Serial-10nF	SATA	ValleyView	SATA_RXP1	-
S75	AFB_DIFF4-	Out	Serial-10nF	SATA	ValleyView	SATA_RXN1	-
-	<Key>	-	-	-	-	-	-
S76	PCIE_B_RST#	Out	-	CMOS 3.3V	CPLD	PMC_PLTRST#	V_1V8_S5
S77	PCIE_C_RST#	Out	-	CMOS 3.3V	CPLD	PMC_PLTRST#	V_1V8_S5
S78	PCIE_C_RX+	In	-	LVDS PCIE	ValleyView	PCIE_RXP2	V_1V0_S0
S79	PCIE_C_RX-	In	-	LVDS PCIE	ValleyView	PCIE_RXN2	V_1V0_S0
S80	GND	-	-	-	-	-	-
S81	PCIE_C_TX+	Out	Serial-100n	LVDS PCIE	ValleyView	PCIE_TXP2	V_1V0_S0
S82	PCIE_C_TX-	Out	Serial-100n	LVDS PCIE	ValleyView	PCIE_TXN2	V_1V0_S0
S83	GND	-	-	-	-	-	-
S84	PCIE_B_REFCK+	Out	-	LVDS PCIE	PEX8605	PCIE_CLKP1	V_1V0_S0
S85	PCIE_B_REFCK-	Out	-	LVDS PCIE	PEX8605	PCIE_CLKN1	V_1V0_S0
S86	GND	-	-	-	-	-	-
S87	PCIE_B_RX+	In	-	LVDS PCIE	ValleyView	PCIE_RXP1	V_1V0_S0
S88	PCIE_B_RX-	In	-	LVDS PCIE	ValleyView	PCIE_RXN1	V_1V0_S0
S89	GND	-	-	-	-	-	-
S90	PCIE_B_TX+	Out	Serial-100n	LVDS PCIE	ValleyView	PCIE_TXP1	V_1V0_S0
S91	PCIE_B_TX-	Out	Serial-100n	LVDS PCIE	ValleyView	PCIE_TXN1	V_1V0_S0
S92	GND	-	-	-	-	-	-
S93	LCD_D0	-	-	-	-	-	-
S94	LCD_D1	-	-	-	-	-	-
S95	LCD_D2	Out	-	CMOS / 1.24V	ValleyView	MCSI_GPIO2	V_1V24_S0
S96	LCD_D3	Out	-	CMOS / 1.24V	ValleyView	MCSI_GPIO3	V_1V24_S0
S97	LCD_D4	Out	-	CMOS / 1.24V	ValleyView	MCSI_GPIO4	V_1V24_S0
S98	LCD_D5	Out	-	CMOS / 1.24V	ValleyView	MCSI_GPIO5	V_1V24_S0
S99	LCD_D6	Out	-	CMOS / 1.24V	ValleyView	MCSI_GPIO8	V_1V24_S0
S100	LCD_D7	Out	-	CMOS / 1.24V	ValleyView	MCSI_GPIO11	V_1V24_S0
S101	GND	-	-	-	-	-	-
S102	LCD_D8	-	-	-	-	-	-
S103	LCD_D9	-	-	-	-	-	-
S104	LCD_D10	-	-	-	-	-	-
S105	LCD_D11	-	-	-	-	-	-
S106	LCD_D12	-	-	-	-	-	-
S107	LCD_D13	Out	-	CMOS / 1.24V	ValleyView	MCSI_GPIO0	V_1V24_S0
S108	LCD_D14	-	-	-	-	-	-
S109	LCD_D15	Out	-	CMOS / 1.24V	ValleyView	MCSI_GPIO1	V_1V24_S0
S110	GND	-	-	-	-	-	-
S111	LCD_D16	-	-	-	-	-	-
S112	LCD_D17	-	-	-	-	-	-
S113	LCD_D18	-	-	-	-	-	-
S114	LCD_D19	-	-	-	-	-	-
S115	LCD_D20	-	-	-	-	-	-
S116	LCD_D21	-	-	-	-	-	-
S117	LCD_D22	-	-	-	-	-	-
S118	LCD_D23	-	-	-	-	-	-
S119	GND	-	-	-	-	-	-
S120	LCD_DE	-	-	-	-	-	-

S121	LCD_VS	-	-	-	-	-	-
S122	LCD_HS	-	-	-	-	-	-
S123	LCD_PCK	Out	Serial-0R	CMOS / 1.8V	ValleyView	PCU_SMB_ALERT#	V_1V8_S0
S124	GND	-	-	-	-	-	-
S125	LVDS0+	Out	-	LVDS LCD	PTN3460B	LVSA0_P	V_1V8_S0
S126	LVDS0-	Out	-	LVDS LCD	PTN3460B	LVSA0_N	V_1V8_S0
S127	LCD_BKLT_EN	Out	-	CMOS / 1.8V	ValleyView	DDI1_BKLTEN	V_1V8_S0
S128	LVDS1+	Out	Serial-0R	LVDS LCD	PTN3460B	LVSB0_P	V_1V8_S0
S129	LVDS1-	Out	Serial-0R	LVDS LCD	PTN3460B	LVSB0_N	V_1V8_S0
S130	GND	-	-	-	-	-	-
S131	LVDS2+	Out	Serial-0R	LVDS LCD	PTN3460B	LVSC0_P	V_1V8_S0
S132	LVDS2-	Out	Serial-0R	LVDS LCD	PTN3460B	LVSC0_N	V_1V8_S0
S133	LCD_VDD_EN	Out	-	CMOS / 1.8V	ValleyView	DDI1_VDDEN	V_1V8_S0
S134	LVDS_CK+	Out	-	LVDS LCD	PTN3460B	LVSCCK_P	V_1V8_S0
S135	LVDS_CK-	Out	-	LVDS LCD	PTN3460B	LVSCCK_N	V_1V8_S0
S136	GND	-	-	-	-	-	-
S137	LVDS3+	Out	-	LVDS LCD	PTN3460B	LVSD0_P	V_1V8_S0
S138	LVDS3-	Out	-	LVDS LCD	PTN3460B	LVSD0_N	V_1V8_S0
S139	I2C_LCD_CK	Out	PU-2k2	CMOS / 1.8V	ValleyView	SIO_I2C2_CLK/_G PIO_S0_SC_82	V_1V8_S0
S140	I2C_LCD_DAT	Bi-Dir	PU-2k2	CMOS / 1.8V	ValleyView	SIO_I2C2_DATA/_ GPIO_S0_SC_83	V_1V8_S0
S141	LCD_BKLT_PWM	Out	-	CMOS / 1.8V	ValleyView	DDI1_BKLTCTL	V_1V8_S0
S142	LCD_DUAL_PCK	-	-	-	-	-	-
S143	GND	-	-	-	-	-	-
S144	RSVD / EDP_HPD	In	-	CMOS / 1.8V	ValleyView	DDI1_HPD	V_1V8_S0
S145	WDT_TIME_OUT#	Out	-	CMOS / 1.8V	ValleyView	GPIO_S0_SC_58	V_1V8_S0
S146	PCIE_WAKE #	In	PU-10k	CMOS 3.3V	ValleyView	PMC_WAKE_PCIE0#	V_3V3_S5
S147	VDD_RTC	-	-	PWR	-	-	-
S148	LID#	In	PU-CPLD-5-25k	CMOS / 1.8V	CPLD	IO_B6	V_1V8_REG_S5
S149	SLEEP#	In	PU-CPLD-5-25k	CMOS / 1.8V	CPLD	IO_A10	V_1V8_REG_S5
S150	VIN_PWR_BAD#	In	PU-CPLD-5-25k	CMOS / 1.8V	CPLD	IO_A2	V_1V8_REG_S5
S151	CHARGING#	In	PU-CPLD-5-25k	CMOS / 1.8V	CPLD	IO_B4	V_1V8_REG_S5
S152	CHARGER_PRSENT#	In	PU-CPLD-5-25k	CMOS / 1.8V	CPLD	IO_B8	V_1V8_REG_S5
S153	CARRIER_STBY#	Out	W-PU-CPLD	CMOS / 1.8V	CPLD	IO_B7	V_1V8_REG_S5
S154	CARRIER_PON	Out	W-PU-CPLD	CMOS / 1.8V	CPLD	IO_A7	V_1V8_REG_S5
S155	FORCE_RECOV#	In	PU-SoC-20k	CMOS / 1.8V	ValleyView	GPIO_S0_SC_56	V_1V8_S0
S156	BATLOW#	In	PU-SoC-20k	CMOS / 1.8V	ValleyView	PMC_BATLOW#	V_1V8_S5
S157	TEST#	In	PU-SoC-20k	CMOS / 1.8V	ValleyView	GPIO_S5_17	V_1V8_S5
S158	VDD_IO_SEL_D#	Bi-Dir	Ground	-	-	-	

7 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.

7.1 Determining the BIOS Version

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

7.2 BIOS Update

Kontron provides continuous BIOS updates for Computer-on-Modules. The updates are provided for download on

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!

7.3 POST Codes

Important POST codes during boot-up

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

7.4 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

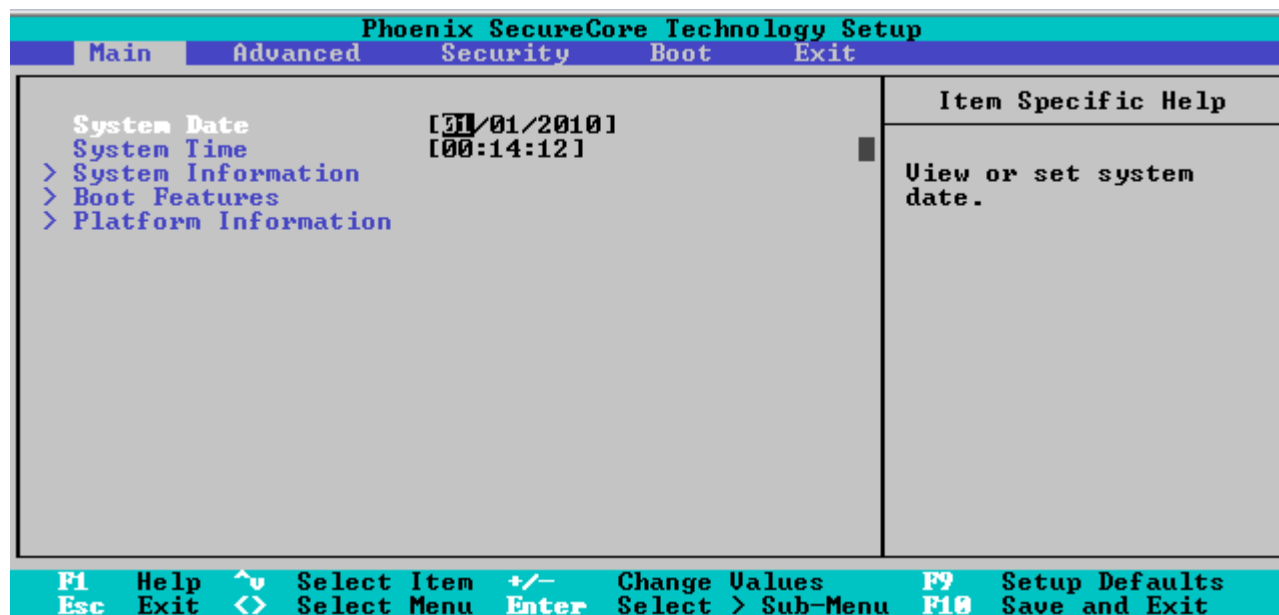
The Help window on the right side of each menu displays the Help text for the selected item. It updates as you move the cursor to each field.

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.

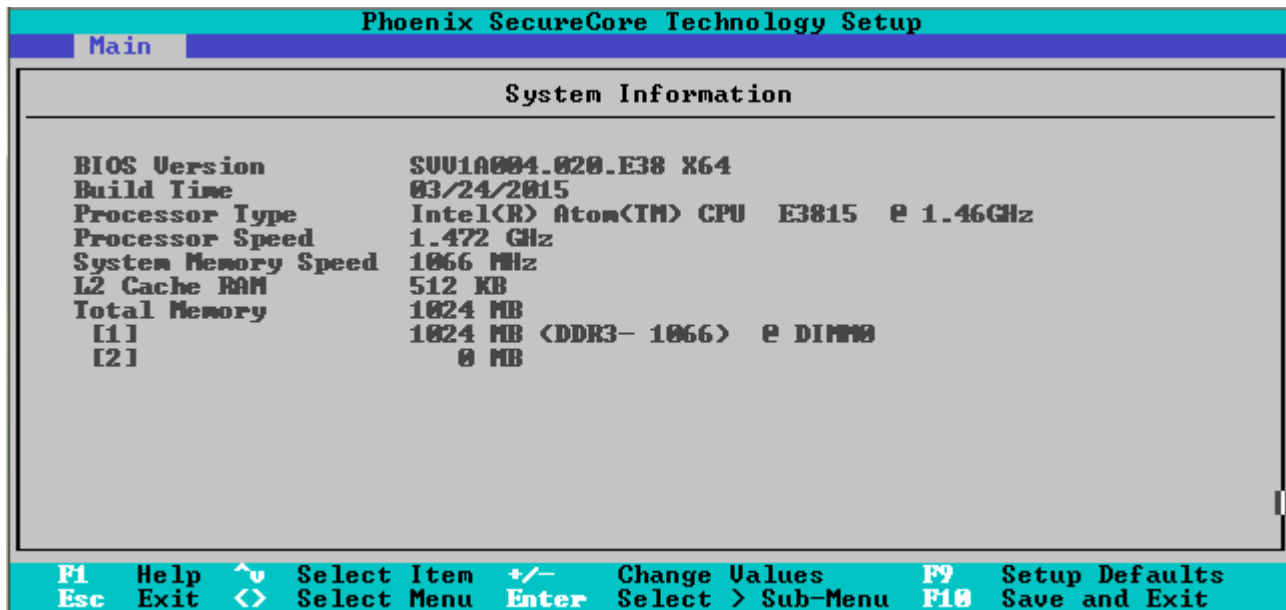
7.5 BIOS Setup

7.5.1 Main



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

System Information



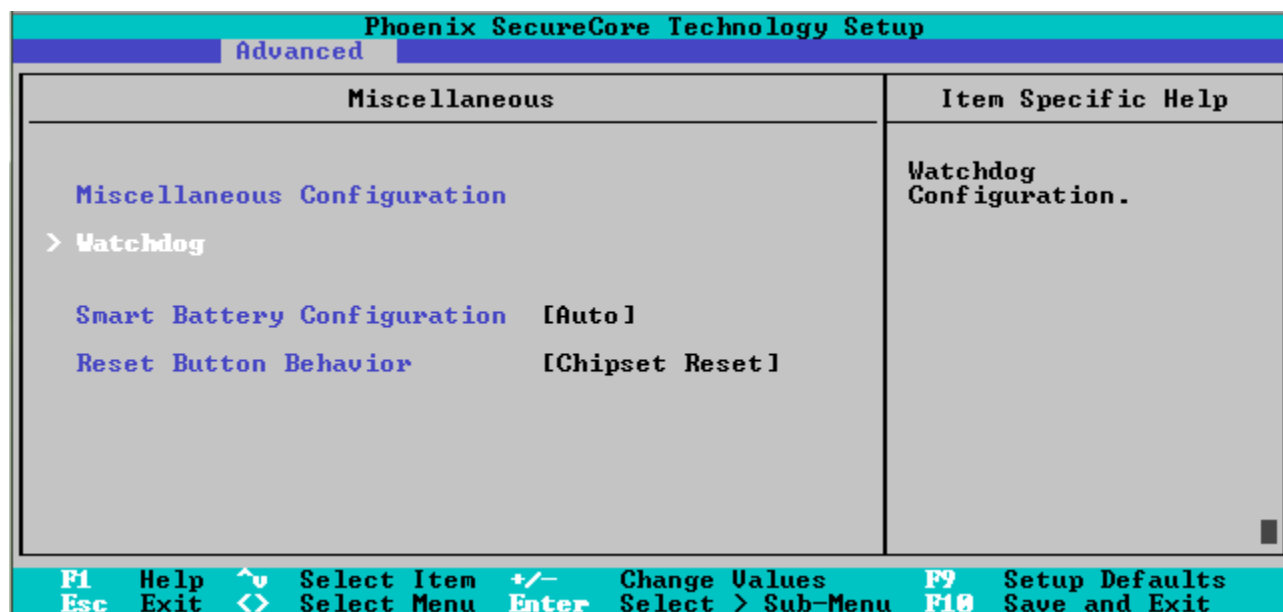
Boot Features

Phoenix SecureCore Technology Setup		
Main		
Boot Features		Item Specific Help
NumLock:	[Off]	Enable/Disable Universal Console Redirection. UCR uses the PCU UART and also requires LPSS HSUART #1 Support to be Disabled. When Console Redirection is Enabled, the PCU UART will be Enabled and HSUART #1 will also be Disabled.
Timeout	[1]	
CSM Support	[Yes]	
Quick Boot	[Disabled]	
Dark Boot	[Disabled]	
Diagnostic Splash Screen	[Disabled]	
Diagnostic Summary Screen	[Disabled]	
BIOS Level USB	[Enabled]	
Console Redirection	[Disabled]	
Allow Hotkey in S4 resume	[Enabled]	
UEFI Boot	[Enabled]	
Legacy Boot	[Enabled]	
Boot in Legacy Video Mode	[Disabled]	
Load OPROM	[On Demand]	
Boot Priority	[UEFI First]	
F1 Help	↑ Select Item	+/- Change Values
Esc Exit	↔ Select Menu	Enter Select > Sub-Menu
		F9 Setup Defaults
		F10 Save and Exit

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
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 RTS/CTS XON/XOFF	Set flow control method for UCR. None = No flow 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 Hibernate state
UEFI Boot	Enabled Disabled	Enable the UEFI boot
Legacy Boot	Enabled	Enable the Legacy boot

	Disabled	
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 OPROM	On Demand All	Load all OPROMs or on demand according to the boot device
Boot Priority	UEFI First Legacy First	Select priority of boot option between UEFI and Legacy

Miscellaneous



Feature	Options	Description
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

Watchdog

Phoenix SecureCore Technology Setup			
Advanced			
Watchdog		Item Specific Help	
Watchdog Configuration. Auto-reload [Disabled] Global Lock [Disabled] API Event [NMI] Stage 1 Mode [Disabled]		Enable automatic reload of watchdog timers on timeout.	
F1 Help ^v Select Item +/- Change Values F9 Setup Defaults Esc Exit <> Select Menu Enter Select > Sub-Menu F10 Save and Exit			

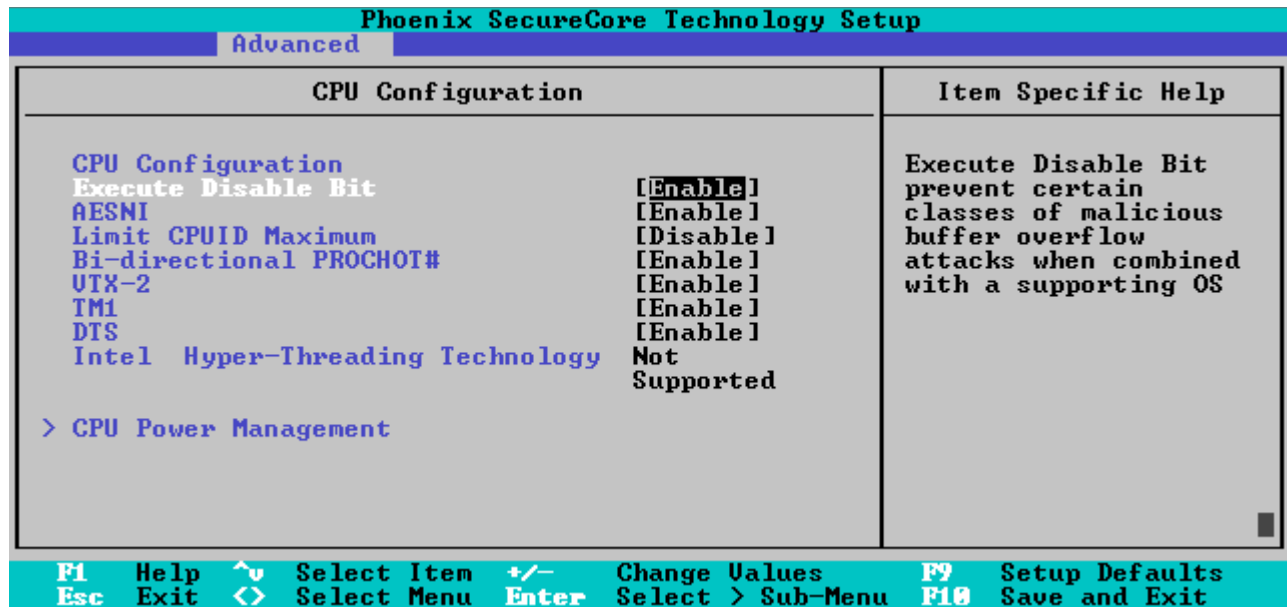
Feature	Options	Description
Auto-reload	Disabled Enabled	Enable automatic reload of watchdog timers on timeout
Global Lock	Disabled Enabled	If set to enabled, all Watchdog registers (except WD_KICK) become read only until the board is reset
API Event	NMI SCI	Select Action for Watchdog if enabled by API.
Stage 1 Mode	Disabled Reset NMI SCI Delay	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

H/W Monitor

Phoenix SecureCore Technology Setup		
Advanced		
H/W Monitor NCT7802Y		Item Specific Help
Temperature Measurement PCB Temperature [+30 C] NCT7802Y Temperature [+30 C] Fan Measurement CPU Fan [N/A] Fan Pulse [2] Fan Control [Auto] Fan Trip Point [45] Trip Point Speed [50] Reference Temperature [PCB Temperature] External Fan [N/A] Fan Pulse [2] Fan Control [Auto] Fan Trip Point [45] Trip Point Speed [50] Reference Temperature [PCB Temperature] Voltage Measurement DDR voltage [+1.37 V] Input voltage [+5.07 V] RTC Battery [+3.60 V]		Number of pulses the fan produces during one revolution. Range: 1-4
Esc Exit <> Select Menu Enter Select > Sub-Menu F10 Save and Exits		

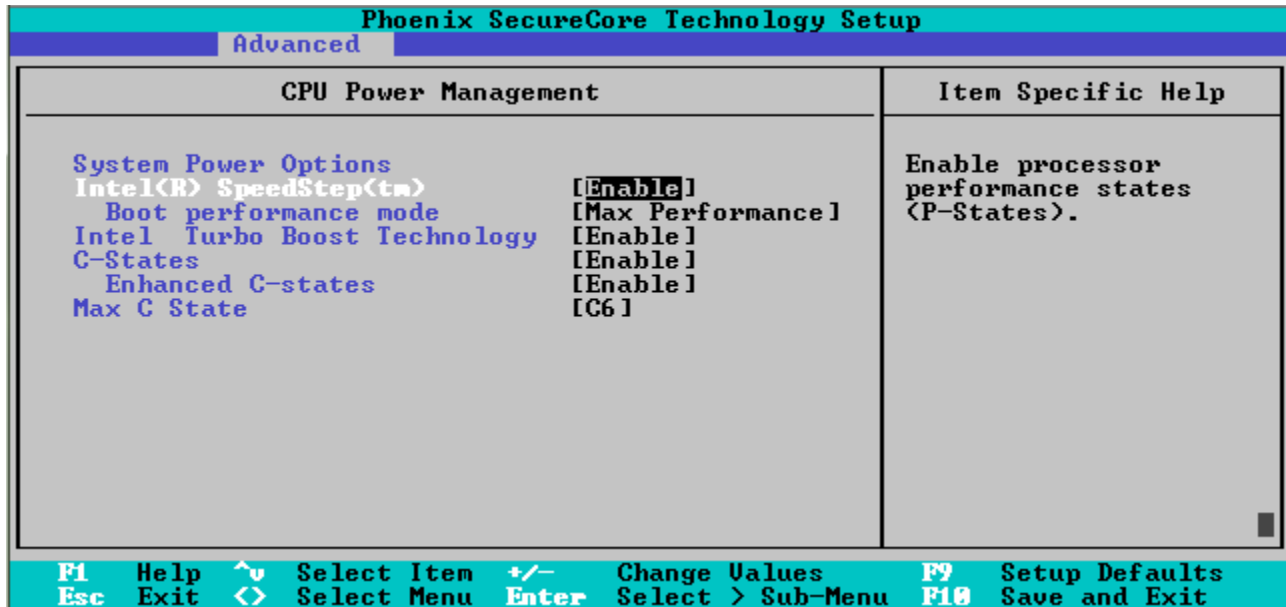
Feature	Value/Options	Description
PCB Temperature	xx°C	Shows the measured temperature of the printed circuit board
NCT782Y Temperature	xx°C	Shows the measured temperature of the NCT782Y Hardware monitor
CPU FAN	xxxx rpm	Shows the fan speed of onboard FAN connector
Fan Pulse	2	Number of pulses the CPU 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
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	PCB Temperature NCT782Y 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
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	PCB Temperature NCT782Y Temperature	Determines the temperature source which is used for automatic fan control
DDR voltage	x.xx V	Shows the Module Main Input Voltage
Input voltage	x.xx V	Shows the 5V Standby Voltage input
RTC battery	x.xx V	Shows the RTC Battery Voltage input measured at COMe connector

CPU Configuration



Feature	Options	Description
Execute Disable Bit	Enable Disable	Execute Disable Bit prevent certain classes of malicious buffer overflow attacks when combined with a supporting OS
AESNI	Enable Disable	Enables or Disables the Advanced Encryption Standards Instruction Set
Limit CPUID Maximum	Enable Disable	Disabled for Windows XP
Bi-directional PROCHOT#	Enable Disable	When a processor thermal sensor trips (either core), the PROCHOT# will be driven. If bi-direction is enabled, external agents can drive PROCHOT# to throttle the processor
VTX-2	Enable Disable	Enables or Disables the VT-x2 Mode support
TM1	Enable Disable	Enables or Disables the Thermal Management 1 support
DTS	Enable Disable	Enables or Disables the Digital Thermal Sensor

CPU Power Management



Feature	Options	Description
Intel® SpeedStep(TM)	Enabled Disabled	Enable/Disable processor performance states (P-States)
Boot Performance Mode	Max Performance Max Battery	Select the performance state that the BIOS sets before OS hand-off
Intel® Turbo Boost Technology	Enabled Disabled	Enable to automatically allow processor cores to run faster than the base operating frequency if it's operating below power, current, and temperature specification limits. This option is only valid for CPUs supporting Intel® Turbo Boost Technology
C-States	Enabled Disabled	Enable processor idle power saving states
Enhanced C-States	Enabled Disabled	Enables or Disables C1E/C2E/C4E. When enabled, CPU will switch to minimum speed when all cores enter C-State
Max C-State	C6 C1	Controls the maximum C-State allowed for the processor

Uncore Configuration

Phoenix SecureCore Technology Setup		
Advanced		
Uncore Configuration		Item Specific Help
IGD Configuration Integrated Graphics Device [Enable] Primary Display [Auto] RC6<Render Standby> [Enable] GTT Size [2MB] Aperture Size [256MB] DVT Pre-Allocated [64M] IGD Turbo [Auto] Spread Spectrum clock [Disable] > IGD - LCD Control		Enable : Enable Integrated Graphics Device (IGD) when selected as the Primary Video Adaptor. Disable: Always disable IGD
F1	Help	^v
Esc	Exit	<>
Select Item		+/-
Select Menu		Enter
Change Values		F9
Select > Sub-Menu		F10
Setup Defaults		
Save and Exit		

Feature	Options	Description
Integrated Graphics Device	Disable Enable	Enable: enable Integrated Graphics Device (IGD) when selected as the Primary Video Adaptor. Disable: Always disable IGD
Primary Display	Auto IGD PCIe SG	Select which of IGD/PCIe Graphics Devices should be Primary Display or select SG for Switchable/Hybrid Graphics
RC6 (Render Standby)	Disable Enable	Enable or Disable Render Standby support
GTT Size	1MB 2MB	Select the GTT Memory Size of IGD
Aperture Size	128MB 256MB 512MB	Select the Graphics Aperture Size
DVMT Pre-Allocated	64M 96M 128M 160M 192M 224M 256M 288M 320M 352M 384M 416M 448M 480M 512M	Select DVMT 5.0 Pre-Allocated (fixed) Graphics Memory size used by the Internal Graphics device
IGD Turbo	Auto Enable Disable	Select the IGD Turbo feature
Spread Spectrum clock	Disable Enable	Enable or Disable clock chip Spread Spectrum feature

IGD - LCD Control

Phoenix SecureCore Technology Setup		
Advanced		
IGD Configuration	Item Specific Help	
IGD managed by: Legacy Video BIOS [3777]	Select the Display Device that should be centered.	
LVDS EEPROM Data Data Format EDID 1.3 Resolution 1280x768 Color Depth 18Bit Channel Count Single Channel		
IGD - Boot Type [EFP] IGD - Secondary Boot Type [LFP]		
LFP Type [Auto] Panel Color Depth [18 Bit] Panel Channel Mode [Single] Backlight Control [PWM] PWM Frequency [200 Hz] Backlight Value [50%] LVDS Clock Center Spreading [No Spreading]		
EFP Type [Auto]		
Mode Persistence [Disabled] Center Mode [Disabled]		
Esc Exit <> Select Menu Enter Select > Sub-Menu F10 Save and Exits		

Feature	Options	Description
IGD - Boot Type	Auto EFP LFP	Select the Integrated Graphics Video Device activated during POST. LFP = Local Flat Panel (LVDS/eDP). EFP = External Flat Panel (Display Port/HDMI)
IGD - Secondary Boot Type	Disabled EFP LFP	Select Secondary Display Device
LFP Type	AUTO VGA 640x480 1x18 WVGA 800x480 1x18 SVGA 800x600 1x18 XGA 1024x768 1x18 XGA 1024x768 1x24 WXGA 1280x768 1x24 WXGA 1280x800 1x18 WXGA 1366x768 1x24 WSVGA 1024x600 1x18 WSVGA 1024x600 1x24 Custom PAID	Select LFP used by Internal Graphics Device by selecting the appropriate panel setup item
Panel Color Depth	18 Bit 24 Bit VESA 24 Bit oLDI	
Panel Channel Mode	Single Dual	Select the Channel Mode of the Panel
Backlight Control	None/External PWM PWM Inverted I2C I2C Inverted	Backlight Control Setting
PWM Frequency	200 hz 400 Hz 1kHz .. 40 kHz	Selects the PWM frequency
Backlight Value	0% .. 50% .. 100%	Set LCD backlight brightness (0-100%)
LVDS Clock Center Spreading	No Spreading 0.5% 1.0%	Select LVDS clock frequency center spreading depth

	1.5% 2.0% 2.5%	
EFP Type	Auto DisplayPort Only DP with HDMI/DVI HDMI/DVI	Integrated HDMI/DisplayPort Configuration with External Connectors
Mode Persistence	Disabled Enabled	Enables/Disables Mode Persistence
Center Mode	Disabled EFP	Select the Display Device that should be centered

South Cluster Configuration

Phoenix SecureCore Technology Setup					
Advanced					
South Cluster Configuration			Item Specific Help		
> PCI Express Configuration > USB Configuration > Audio Configuration > SATA Drives > LPSS & SCC Configuration > Miscellaneous Configuration			PCI Express Configuration Settings		
F1	Help	↑	Select Item	+/-	Change Values
Esc	Exit	<>	Select Menu	Enter	Select > Sub-Menu
F9	Setup Defaults				F10
				Save and Exit	

PCI Express Configuration

Phoenix SecureCore Technology Setup	
Advanced	
PCI Express Configuration	Item Specific Help
PCIe 0 Speed [Auto] PCIe 1 Speed [Auto] PCIe 2 Speed [Auto] PCIe 3 Speed [Auto] PCI Express Root Port 0 [Enable] PCI Express Root Port 1 [Enable] PCI Express Root Port 2 [Enable] PCI Express Root Port 3 [Enable]	Configure PCIe Speed
F1 Help ^v Select Item +/- Change Values F9 Setup Defaults Esc Exit <> Select Menu Enter Select > Sub-Menu F10 Save and Exit	

Feature	Options	Description
PCIe Speed	Auto Gen1 Gen2	Select PCIe Speed to Gen1 or Gen2
PCI Express Root Port	Disable Enable	Control the PCI Express Root Port

USB Configuration

Phoenix SecureCore Technology Setup		
Advanced		
USB Configuration		Item Specific Help
xHCI Mode [Enable] EHCI Controller [Disable] USB Per-Port Control [Enable] USB Port #0 [Enable] USB Port #1 [Enable] USB Port #2 [Enable] USB Port #3 [Enable] XHCI Link Power Management [Disable] USB Port Power Enable/Disable USB0 Power Enable [Enabled] USB1 Power Enable [Enabled] USB2 Power Enable [Enabled] USB3 Power Enable [Enabled] USB Port Wake Enable/Disable USB0 Wake Enable [Enabled] USB1 Wake Enable [Enabled] USB2 Wake Enable [Enabled] USB3 Wake Enable [Enabled] USB 0 Host/Client mode [Host mode]		Mode of operation of xHCI controller. This will also influence EHCI controller settings since certain combinations of those modes are not allowed. 'Smart Auto' mode is supposed to solve USB issues under Windows 7
F1 Help ↑ Select Item +/- Change Values F9 Setup Defaults Esc Exit <> Select Menu Enter Select > Sub-Menu F10 Save and Exit		

Feature	Options	Description
xHCI Mode	Smart Auto Enable Disable	Mode of operation of xHCI controller. This will also influence EHCI controller settings since certain combinations of those modes are not allowed. 'SMART Auto' Mode is required for OS with external Driver (e.g. Windows 7), 'Enabled' is recommended for OS with integrated USB 3.0 Support (e.g. Windows 8). Please note, the USB HSIC Hub for COMe USB Ports #4-7 is linked to xHCI controller which allows operation of these USB ports in OS with USB 3.0 driver only (no support in DOS or EFI Shell)
XHCI Link Power Management	Disable Enable	Enable/Disable XHCI Link Power Management
USB Per-Port Control	Disable Enable	Controls each of the CPU USB ports (COMe USB #0-3)
- USB Port #0 - USB Port #1 - USB Port #2 - USB Port #3	Disabled Enabled	Enable/Disable USB port
USB 0 Host/Client mode	Host mode Client mode	Selects the USB mode for USB 0

Audio Configuration

Phoenix SecureCore Technology Setup		
Advanced		
Audio Configuration		Item Specific Help
Audio Configuration Audio Controller [Enable] HDAudio VCI Enable [Enable] HDAudio Docking Support Enable [Disable] HDAudio PME Enable [Enable] HDAudio HDMI Codec [Enable]		Control Detection of the HDAudio device. Disabled = Azalia will be unconditionally disabled Enabled = Azalia will be unconditionally Enabled Auto = Azalia will be enabled if present, disabled otherwise
F1 Help ^v Select Item +/- Change Values F9 Setup Defaults Esc Exit <> Select Menu Enter Select > Sub-Menu F10 Save and Exit		

Feature	Options	Description
Audio Controller	Enable Disable	Enable / Disable High Definition Audio interface
- HDAudio VCI Enable	Enable Disable	Enable / Disable Virtual Channel 1 of Audio Controller
- HDAudio Docking Support Enable	Enable Disable	Enable / Disable HDAudio Docking Support of Audio Controller
- HDAudio PMCE Enable	Enable Disable	Enable / Disable Power Management capability of Audio Controller
- HDAudio HDMI Codec	Enable Disable	Enable / Disable internal HDMI codec for HDAudio

SATA Drives

Phoenix SecureCore Technology Setup	
Advanced	
SATA Drives	Item Specific Help
SATA Drives Chipset-SATA Controller Configuration Chipset SATA [Enable] SATA Test Mode [Disable] Chipset SATA Mode [AHCI] SATA Port 0 Hot Plug Capability [Disable] SATA Port 1 Hot Plug Capability [Disable]	Enables or Disables the Chipset SATA Controller. The Chipset SATA controller supports the 2 black internal SATA ports (up to 3Gb/s supported per port).
F1 Help ↑ Select Item +/- Change Values F9 Setup Defaults Esc Exit <> Select Menu Enter Select > Sub-Menu F10 Save and Exit	

Feature	Options	Description
Chipset SATA	Enable Disable	Enables or Disables the Chipset SATA Controller. The Chipset SATA controller supports the 2 internal SATA ports (up to 3Gb/s supported per port)
SATA Test Mode	Disable Enable	Enables or Disables the SATA Test Mode
Chipset SATA Mode	IDE AHCI	IDE: compatibility mode, disables AHCI. AHCI: supports advanced SATA features such as NCQ. Warning: do not change after OS install
SATA Port 0 Hot Plug Capability	Enable Disable	If enabled, SATA port will be reported as HotPlug capable
SATA Port 1 Hot Plug Capability	Enable Disable	If enabled, SATA port will be reported as HotPlug capable

LPSS & SCC Configuration

Phoenix SecureCore Technology Setup		
Advanced		
LPSS & SCC Configuration		Item Specific Help
LPSS & SCC Devices Mode [PCI Mode] SCC Configuration SCC eMMC Boot Controller [Auto Detect] eMMC 4.5 Support [Enable] eMMC DDR50 Support [Disable] eMMC HS200 Support [Disable] eMMC retune timer value [8] SCC SD Card Support [Enable] SD SDR 25 Support [Enable] SD SDR 50 Support [Disable] SCC SDIO Support [Disable] MIPI HSI Support [Disable] LPSS Configuration LPSS DMA #1 Support [Enable] LPSS DMA #2 Support [Enable] LPSS I2C #1 Support [Enable] LPSS I2C #2 Support [Enable] LPSS I2C #3 Support [Enable] LPSS I2C #4 Support [Enable] LPSS I2C #5 Support [Enable] LPSS I2C #6 Support [Disable] LPSS I2C #7 Support [Disable] LPSS HSUART #1 Support [Enable] LPSS HSUART #2 Support [Enable]		LPSS & SCC Devices Mode Settings. Use ACPI mode for Windows 8 and use PCI mode for Windows 7.
F1 Help Esc Exit ↩ Select Item +/- Change Values F9 Setup Defaults ↪ Select Menu Enter Select > Sub-Menu F10 Save and Exit		

Feature	Options	Description
LPSS & SCC Devices Mode	ACPI Mode PCI Mode	Select operation mode for Low Power Super Speed LPSS devices eMMC/SDCard. For eMMC full speed operation the LPSS mode should be set to "ACPI"
SCC eMMC Boot Controller	Disable Auto Detect eMMC 4.41 eMMC 4.5	Disable or select eMMC Boot mode
eMMC 4.5 support	Disable Enable	Enabled: eMMC 4.5, Disabled: eMMC 4.41
eMMC DDR50 Support	Disable Enable	Enable / Disable DDR50 speed mode for eMMC
eMMC HS200 Support	Disable Enable	Enable / Disable HS200 speed mode for eMMC. For eMMC full speed operation the HS200 mode should be enabled.
- eMMC retune timer value	8	Select the retune timer in HS200 mode
SCC SD Card Support	Disable Enable	Enable / Disable SD Card Support
SD SDR 25 Support	Disable Enable	Enable bus speed operation up to 25MB/s for SDCard (High Speed). Disable limits bus speed to 12.5MB/s (normal speed)
SD SDR 50 Support	Disable Enable	Enable bus speed operation up to 50MB/s for SDCard (Ultra High Speed). Disabled activates SDR25 mode setting
SD SDIO Support	Disable Enable	Enable / Disable SD SDIO Support
MIPI HSI Support	Disable Enable	Enable / Disable MIPI HSI Support
LPSS DMA #X	Disable Enable	Enable / Disable LPSS DMA Channel #X
LPSS I2C #X (1-5)	Disable Enable	Enable / Disable LPSS I2C Channel #X
LPSS I2C #X (6-7)	Disable Enable	Enable / Disable LPSS I2C Channel #X
LPSS HSUART #X	Disable Enable	Enable / Disable LPSS High Speed UART Channel #X

Miscellaneous Configuration

Phoenix SecureCore Technology Setup		
Advanced		
Miscellaneous Configuration		Item Specific Help
Miscellaneous Configuration High Precision Timer [Enable] Boot Time with HPET Timer [Disable] State After G3 [S0 State] Clock Spread Spectrum [Disable] SMM LOCK [Enable] Pci Mmio Size [2GB] PXE ROM [Disabled]		Enable or Disable the High Precision Event Timer
F1 Help ^v Select Item +/- Change Values F9 Setup Defaults Esc Exit <> Select Menu Enter Select > Sub-Menu F10 Save and Exit		

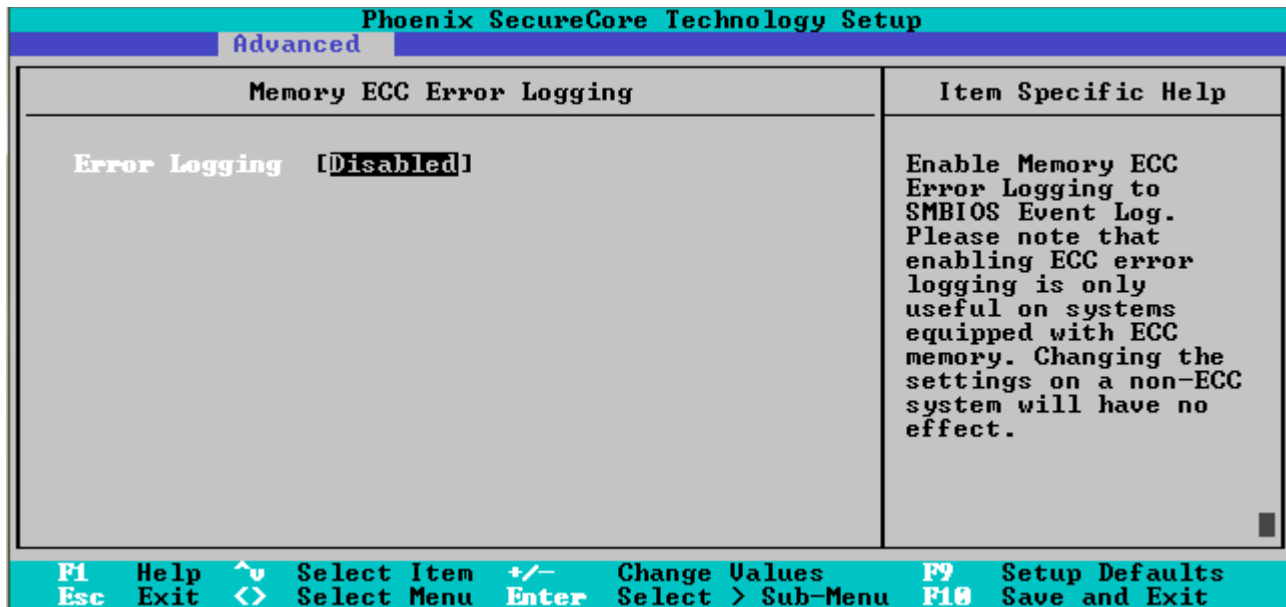
Feature	Options	Description
High Precision Timer	Disable Enable	Enables or Disables the High Precision Event Timer
Boot Time with HPET Timer	Disable Enable	Boot time calculation with High Precision Event Timer enabled
State After G3	S0 State S5 State	Specify what state to go to when power is re-applied after a power failure (G3 state). S0 = Power on, S5 = Stay off
Clock Spread Spectrum	Disable Enable	Enables or Disables the Clock Spread Spectrum
SMM LOCK	Disable Enable	Enables or Disables the SMM Lock feature. It will lock the SMRAM and unable load SMM driver any more
PCI Mmio Size	2GB 1.5GB 1.25GB 1GB	Selects the PCI Mmio Size
PXE ROM	Disable Enable	Enables or Disables the PXE Boot ROM

SMBIOS Event Log

Phoenix SecureCore Technology Setup		
Advanced		
SMBIOS Event Log		Item Specific Help
Event Log Validity	Valid	Enable/Disable Event Log.
Event Log Capacity	Space Available	
Event Log	[Disabled]	
> View SMBIOS event log		
Mark SMBIOS events as read	[Enter]	
Clears SMBIOS events	[Enter]	
F1 Help ↑ Select Item +/- Change Values F9 Setup Defaults Esc Exit <> Select Menu Enter Select > Sub-Menu F10 Save and Exit		

Feature	Options	Description
Event Log	Disable Enable	Enables or Disables the SMBIOS Event Log
Mark SMBIOS events as read	Enter	Mark SMBIOS events as read. Marked SMBIOS events won't be displayed
Clears SMBIOS events	Enter	Clear SMBIOS events

Memory ECC Error Logging



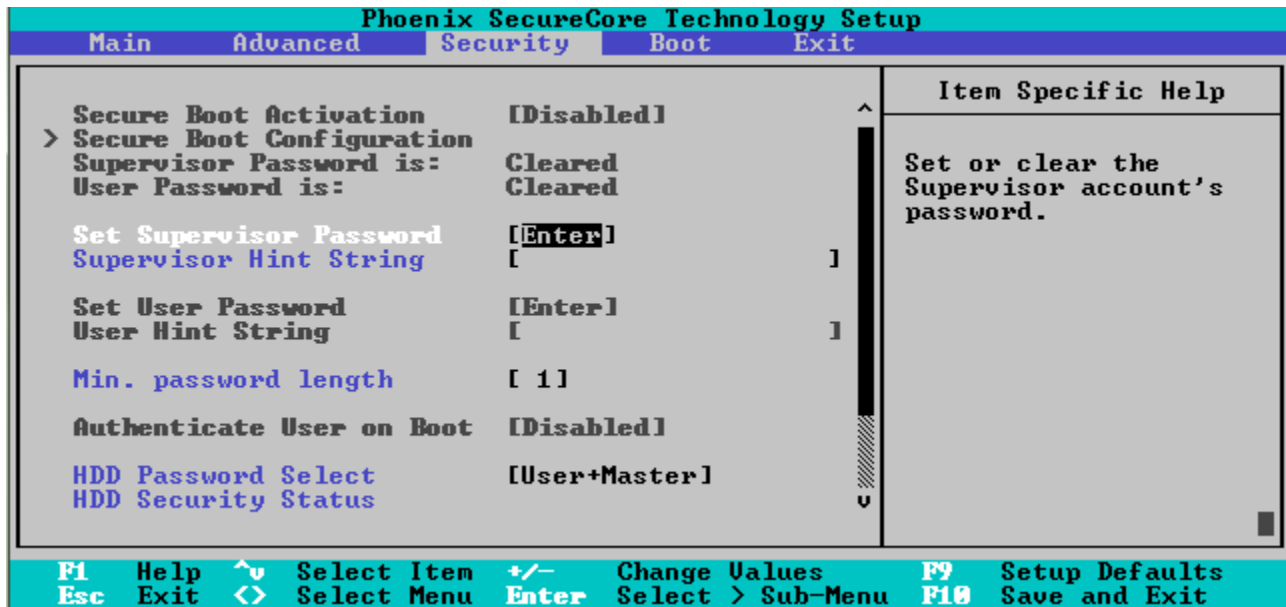
Feature	Options	Description
Error Logging	Disabled Enabled	Enable Memory ECC Error Logging to SMBIOS Event Log. Please note that enabling ECC error logging is only useful on systems equipped with ECC memory. Changing the settings on a non-ECC system will have no effect
- Single-Bit	Disabled Enabled	Log single bit errors
- SECC Threshold	Disabled Enabled	When the error times exceeds the threshold counter every time, then to record the event
- SECC Threshold Counter	20	Range from Min. to Max. (0 65535)
- Multi-Bit	Disabled Enabled	Log multi bit errors
- Halt on Uncorrectable Error	Disabled Enabled	Controls whether to halt or not when uncorrectable errors are encountered

Kontron Board

Phoenix SecureCore Technology Setup		
Advanced		
Kontron Board	Item Specific Help	
Sleep and Wake settings Wake on LAN [Disabled] S5 Eco [Disabled] SMBus and I2C bus control SMBus S0-S5 [Disabled] SMBus-I2CPM [Enabled] I2CPM-I2CPMEXT [Enabled] GPIO Mux Enable/Disable GPIO MUX0 Select [Serial Camera 0 Con] GPIO MUX1 Select [Serial Camera 1 Con] GPIO MUX2 Select [HDA Audio Enabled] GPIO MUX3 Select [FAN Control Enabled] SMARC GPIO Settings SMARC GPIO07 Mode [Input] SMARC GPIO08 Mode [Input] SMARC GPIO09 Mode [Input] SMARC GPIO10 Mode [Input] SMARC GPIO11 Mode [Input]	Wake on LAN Enable or Disable.	
F1 Help ^v Select Item +/- Change Values F9 Setup Defaults Esc Exit <> Select Menu Enter Select > Sub-Menu F10 Save and Exit		

Feature	Options	Description
Wake on LAN	Disabled Enabled	Enable or Disable Wake on LAN
S5 Eco	Disabled Enabled	Enable or Disable S5 Eco
SMB S0-S5	Disabled Enabled	Enable or Disable SMB S0-S5
SMB-I2CPM	Disabled Enabled	Enable or Disable I2CPM
I2CPM-I2CPMEXT	Disabled Enabled	Enable or Disable I2CPMEXT
GPIO MUX 0 Select	3 4 5 6 7 12	Configure Serial Port IRQ

7.5.3 Security



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

TPM Options

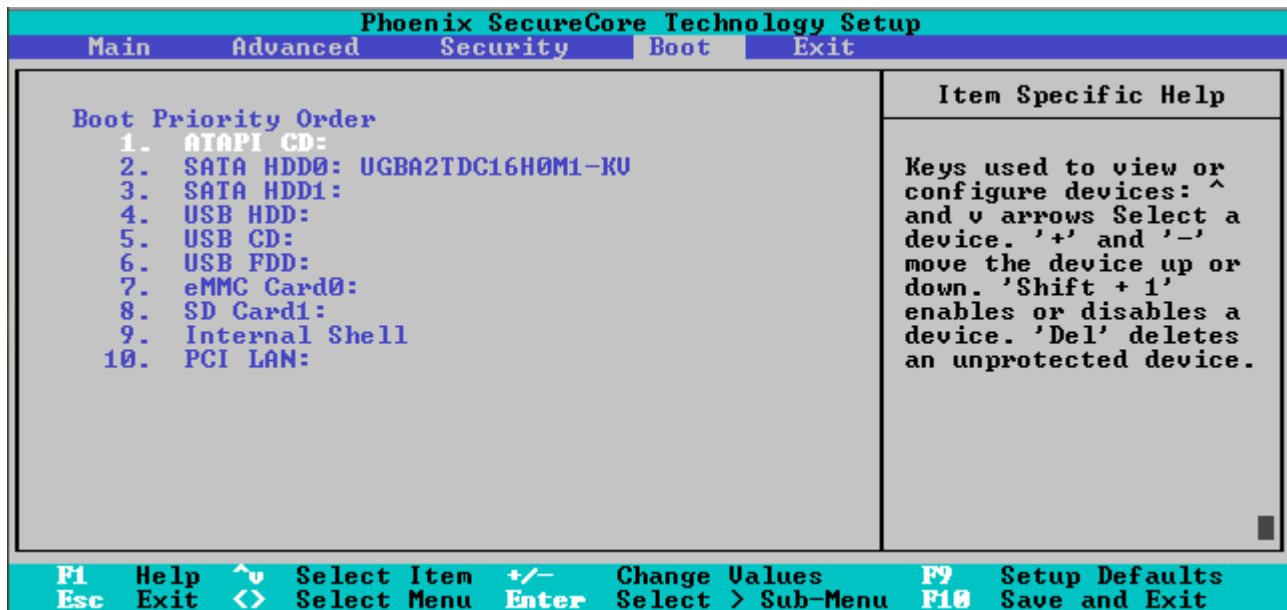
Feature	Options	Description
TPM Action	No Change Enable Disable Activate Deactivate Clear Enable and Activate Disable and Deactivate Set Owner Install, with state=True Set Owner Install, with state=False Enable, Activate, and Set Owner Install with state=True Disable, Deactivate, and Set Owner Install 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]

Secure Boot

Phoenix SecureCore Technology Setup		
Security		
Secure Boot Configuration		Item Specific Help
UEFI Secure Boot	Disabled	Enable or disable secure boot function.
Protected Signatures	Disabled (Setup Mode)	
Customized Signatures	Disabled (Standard Mode)	
CertNames	Win8 Certificates	
Secure Boot Option	[Enabled]	
Reset to Default	[Enter]	
Change to Customization	[Enter]	
F1 Help ^v Select Item +/- Change Values F9 Setup Defaults Esc Exit <> Select Menu Enter Select > Sub-Menu F10 Save and Exit		

Feature	Options	Description
Secure Boot Option	Enabled Disabled	Set or clear the Supervisor account's password
Reset to Default	Enter	Reset Secure Boot options to manufacturing defaults
Change to customization	Enter	PK will be deleted, the platform will be changed to setup mode, and secure boot is disabled automatically.

7.5.4 Boot



7.5.5 Exit

