USER GUIDE

QSEVEN-Q7ALx2

Doc. User Guide, Rev. 1.0

Doc. ID: 1067-2270

This page has been intentionally left blank

QSEVEN-Q7ALX2 - USER GUIDE

Disclaimer

Kontron would like to point out that the information contained in this user guide may be subject to alteration, particularly as a result of the constant upgrading of Kontron products. This document does not entail any guarantee on the part of Kontron with respect to technical processes described in the user guide or any product characteristics set out in the user guide. Kontron assumes no responsibility or liability for the use of the described product(s), conveys no license or title under any patent, copyright or mask work rights to these products and makes no representations or warranties that these products are free from patent, copyright or mask work right infringement unless otherwise specified. Applications that are described in this user guide are for illustration purposes only. Kontron makes no representation or warranty that such application will be suitable for the specified use without further testing or modification. Kontron expressly informs the user that this user guide only contains a general description of processes and instructions which may not be applicable in every individual case. In cases of doubt, please contact Kontron.

Kontron Europe GmbH

Gutenbergstrasse 2
85737 Ismaning
Germany
www.kontron.com

Intended Use

THIS DEVICE AND ASSOCIATED SOFTWARE ARE NOT DESIGNED, MANUFACTURED OR INTENDED FOR USE OR RESALE FOR THE OPERATION OF NUCLEAR FACILITIES, THE NAVIGATION, CONTROL OR COMMUNICATION SYSTEMS FOR AIRCRAFT OR OTHER TRANSPORTATION, AIR TRAFFIC CONTROL, LIFE SUPPORT OR LIFE SUSTAINING APPLICATIONS, WEAPONS SYSTEMS, OR ANY OTHER APPLICATION IN A HAZARDOUS ENVIRONMENT, OR REQUIRING FAIL-SAFE PERFORMANCE, OR IN WHICH THE FAILURE OF PRODUCTS COULD LEAD DIRECTLY TO DEATH, PERSONAL INJURY, OR SEVERE PHYSICAL OR ENVIRONMENTAL DAMAGE (COLLECTIVELY, "HIGH RISK APPLICATIONS").

You understand and agree that your use of Kontron devices as a component in High Risk Applications is entirely at your risk. To minimize the risks associated with your products and applications, you should provide adequate design and operating safeguards. You are solely responsible for compliance with all legal, regulatory, safety, and security related requirements concerning your products. You are responsible to ensure that your systems (and any Kontron hardware or software components incorporated in your systems) meet all applicable requirements. Unless otherwise stated in the product documentation, the Kontron device is not provided with error-tolerance capabilities and cannot therefore be deemed as being engineered, manufactured or setup to be compliant for implementation or for resale as device in High Risk Applications. All application and safety related information in this document (including application descriptions, suggested safety measures, suggested Kontron products, and other materials) is provided for reference only.

Revision History

Revision	Brief Description of Changes	Date of Issue	Author
1.0	Initial version	2020-Dec-16	CW

Terms and Conditions

Kontron warrants products in accordance with defined regional warranty periods. For more information about warranty compliance and conformity, and the warranty period in your region, visit http://www.kontron.com/terms-and-conditions.

Kontron sells products worldwide and declares regional General Terms & Conditions of Sale, and Purchase Order Terms & Conditions. Visit http://www.kontron.com/terms-and-conditions.

For contact information, refer to the corporate offices contact information on the last page of this user guide or visit our website CONTACT US.

Customer Support

Find Kontron contacts by visiting: http://www.kontron.com/support.

Customer Service

As a trusted technology innovator and global solutions provider, Kontron extends its embedded market strengths into a services portfolio allowing companies to break the barriers of traditional product lifecycles. Proven product expertise coupled with collaborative and highly-experienced support enables Kontron to provide exceptional peace of mind to build and maintain successful products.

For more details on Kontron's service offerings such as: enhanced repair services, extended warranty, Kontron training academy, and more visit http://www.kontron.com/support-and-services/services.

Customer Comments

If you have any difficulties using this user guide, discover an error, or just want to provide some feedback, contact Kontron Support. Detail any errors you find. We will correct the errors or problems as soon as possible and post the revised user guide on our website.

Symbols

The following symbols may be used in this user guide

⚠DANGER	DANGER indicates a hazardous situation which, if not avoided, will result in death or serious injury.
⚠WARNING	WARNING indicates a hazardous situation which, if not avoided, could result in death or serious injury.
NOTICE	NOTICE indicates a property damage message.
⚠CAUTION	CAUTION indicates a hazardous situation which, if not avoided, may result in minor or moderate injury.
⚡	Electric Shock! This symbol and title warn of hazards due to electrical shocks (> 60 V) when touching products or parts of products. Failure to observe the precautions indicated and/or prescribed by the law may endanger your life/health and/or result in damage to your material.
⚠	ESD Sensitive Device! This symbol and title inform that the electronic boards and their components are sensitive to static electricity. Care must therefore be taken during all handling operations and inspections of this product in order to ensure product integrity at all times.
⚠	HOT Surface! Do NOT touch! Allow to cool before servicing.
⚠	Laser! This symbol inform of the risk of exposure to laser beam and light emitting devices (LEDs) from an electrical device. Eye protection per manufacturer notice shall review before servicing.
▶ i	This symbol indicates general information about the product and the user guide. This symbol also indicates detail information about the specific product configuration.
💡	This symbol precedes helpful hints and tips for daily use.

For Your Safety

Your new Kontron product was developed and tested carefully to provide all features necessary to ensure its compliance with electrical safety requirements. It was also designed for a long fault-free life. However, the life expectancy of your product can be drastically reduced by improper treatment during unpacking and installation. Therefore, in the interest of your own safety and of the correct operation of your new Kontron product, you are requested to conform with the following guidelines.

High Voltage Safety Instructions

As a precaution and in case of danger, the power connector must be easily accessible. The power connector is the product's main disconnect device.

⚠CAUTION

Warning

All operations on this product must be carried out by sufficiently skilled personnel only.

⚠CAUTION

Electric Shock!

Before installing a non hot-swappable Kontron product into a system always ensure that your mains power is switched off. This also applies to the installation of piggybacks. Serious electrical shock hazards can exist during all installation, repair, and maintenance operations on this product. Therefore, always unplug the power cable and any other cables which provide external voltages before performing any work on this product.

Earth ground connection to vehicle's chassis or a central grounding point shall remain connected. The earth ground cable shall be the last cable to be disconnected or the first cable to be connected when performing installation or removal procedures on this product.

Special Handling and Unpacking Instruction

NOTICE

ESD Sensitive Device!

Electronic boards and their components are sensitive to static electricity. Therefore, care must be taken during all handling operations and inspections of this product, in order to ensure product integrity at all times.

⚠CAUTION

Handling and operation of the product is permitted only for trained personnel within a work place that is access controlled. Follow the "General Safety Instructions for IT Equipment" supplied with the product.

Do not handle this product out of its protective enclosure while it is not used for operational purposes unless it is otherwise protected.

Whenever possible, unpack or pack this product only at EOS/ESD safe work stations. Where a safe work station is not guaranteed, it is important for the user to be electrically discharged before touching the product with his/her hands or tools. This is most easily done by touching a metal part of your system housing.

It is particularly important to observe standard anti-static precautions when changing piggybacks, ROM devices, jumper settings etc. If the product contains batteries for RTC or memory backup, ensure that the product is not placed on conductive surfaces, including anti-static plastics or sponges. They can cause short circuits and damage the batteries or conductive circuits on the product.

Lithium Battery Precautions

If your product is equipped with a lithium battery, take the following precautions when replacing the battery.

⚠CAUTION

Danger of explosion if the battery is replaced incorrectly.

- Replace only with same or equivalent battery type recommended by the manufacturer.
- Dispose of used batteries according to the manufacturer's instructions.

General Instructions on Usage

In order to maintain Kontron's product warranty, this product must not be altered or modified in any way. Changes or modifications to the product, that are not explicitly approved by Kontron and described in this user guide or received from Kontron Support as a special handling instruction, will void your warranty.

This product should only be installed in or connected to systems that fulfill all necessary technical and specific environmental requirements. This also applies to the operational temperature range of the specific board version that must not be exceeded. If batteries are present, their temperature restrictions must be taken into account.

In performing all necessary installation and application operations, only follow the instructions supplied by the present user guide.

Keep all the original packaging material for future storage or warranty shipments. If it is necessary to store or ship the product then re-pack it in the same manner as it was delivered.

Special care is necessary when handling or unpacking the product. See Special Handling and Unpacking Instruction.

Quality and Environmental Management

Kontron aims to deliver reliable high-end products designed and built for quality, and aims to complying with environmental laws, regulations, and other environmentally oriented requirements. For more information regarding Kontron's quality and environmental responsibilities, visit http://www.kontron.com/about-kontron/corporate-responsibility/quality-management.

Disposal and Recycling

Kontron's products are manufactured to satisfy environmental protection requirements where possible. Many of the components used are capable of being recycled. Final disposal of this product after its service life must be accomplished in accordance with applicable country, state, or local laws or regulations.

WEEE Compliance

The Waste Electrical and Electronic Equipment (WEEE) Directive aims to:

- Reduce waste arising from electrical and electronic equipment (EEE)
- Make producers of EEE responsible for the environmental impact of their products, especially when the product is waste
- Encourage separate collection and subsequent treatment, reuse, recovery, recycling and sound environmental disposal of EEE
- Improve the environmental performance of all those involved during the lifecycle of EEE

Environmental protection is a high priority with Kontron.
Kontron follows the WEEE directive
You are encouraged to return our products for proper disposal.

Table of Contents

List of Tables

List of Figures

1/ Introduction

This user guide describes the Qseven® Q7ALx2 module from Kontron. The Q7ALx2 is an off-the-shelf module designed to meet the Qseven® standard. The use of the Qseven® Q7ALx2 module requires basic knowledge of PC hardware and software. This user guide focuses on describing the Q7ALx2's special features and is not intended to be a standard PC textbook.

Before powering on the Q7ALx2 module, Kontron recommends new users to read and observe Chapter 2/: General Safety Instructions, and study the power on procedure in Chapter 9/: Power on.

The configuration and setup of the Qseven® Q7ALx2 module is automatic, or performed manually by the user within the BIOS setup.

Latest revision of this user guide, datasheet, BIOS, drivers and BSPs (Board Support Packages) are available for downloaded from Kontron's Web Page.

2/ General Safety Instructions

Please read this passage carefully and take careful note of the instructions, which have been compiled for your safety and to ensure to apply in accordance with intended regulations. If the following general safety instructions are not observed, it could lead to injuries to the operator and/or damage of the product; in cases of non-observance of the instructions Kontron Europe is exempt from accident liability, this also applies during the warranty period.

The product has been built and tested according to the basic safety requirements for low voltage (LVD) applications and has left the manufacturer in safety-related, flawless condition. To maintain this condition and to also ensure safe operation, the operator must not only observe the correct operating conditions for the product but also the following general safety instructions:

- The product must be used as specified in the product documentation, in which the instructions for safety for the product and for the operator are described. These contain guidelines for setting up, installation and assembly, maintenance, transport or storage.
- The on-site electrical installation must meet the requirements of the country's specific local regulations.
- If a power cable comes with the product, only this cable should be used. Do not use an extension cable to connect the product.
- To guarantee that sufficient air circulation is available to cool the product, please ensure that the ventilation openings are not covered or blocked. If a filter mat is provided, this should be cleaned regularly. Do not place the product close to heat sources or damp places. Make sure the product is well ventilated.
- Only connect the product to an external power supply providing the voltage type (AC or DC) and the input power (max. current) specified on the Kontron Product Label and meeting the requirements of the Limited Power Source (LPS) and Power Source (PS2) of UL/IEC 62368-1 .
- Only products or parts that meet the requirements for Power Source (PS1) of UL/IEC 62368-1 may be connected to the product's available interfaces (I/O).
- Before opening the product, make sure that the product is disconnected from the mains.
- Switching off the product by its power button does not disconnect it from the mains. Complete disconnection is only possible if the power cable is removed from the wall plug or from the product. Ensure that there is free and easy access to enable disconnection.
- The product may only be opened for the insertion or removal of add-on cards (depending on the configuration of the product). This may only be carried out by qualified operators.
- If extensions are being carried out, the following must be observed:
  - all effective legal regulations and all technical data are adhered to
  - the power consumption of any add-on card does not exceed the specified limitations
  - the current consumption of the product does not exceed the value stated on the product label.
- Only original accessories that have been approved by Kontron Europe can be used.
- Please note: safe operation is no longer possible when any of the following applies:
  - the product has visible damages or
  - the product is no longer functioning

    In this case the product must be switched off and it must be ensured that the product can no longer be operated.
- Handling and operation of the product is permitted only for trained personnel within a work place that is access controlled.
- CAUTION: Risk of explosion if the battery is replaced incorrectly (short-circuited, reverse-poled, wrong battery type). Dispose of used batteries according to the manufacturer's instructions.
- This product is not suitable for use in locations where children are likely to be present

Additional Safety Instructions for DC Power Supply Circuits

- To guarantee safe operation, please observe that:
  - the external DC power supply must meet the criteria for LPS and PS2 (UL/IEC 62368-1)
  - no cables or parts without insulation in electrical circuits with dangerous voltage or power should be touched directly or indirectly
  - a reliable protective earthing connection is provided

  - a suitable, easily accessible disconnecting device is used in the application (e.g. overcurrent protective device), if the product itself is not disconnect able
  - a disconnect device, if provided in or as part of the product, shall disconnect both poles simultaneously
  - interconnecting power circuits of different products cause no electrical hazards
- A sufficient dimensioning of the power cable wires must be selected – according to the maximum electrical specifications on the product label – as stipulated by EN62368-1 or VDE0100 or EN60204 or UL61010-1 regulations.

2.1. Electrostatic Discharge (ESD)

A sudden discharge of electrostatic electricity can destroy static-sensitive devices.

Proper packaging and grounding techniques are necessary precautions to prevent damage. Always take the following precautions:

1. Transport ESD-sensitive products in ESD-safe containers such as boxes or bags.
2. Keep electrostatic sensitive parts in their containers until they arrive at the ESD-safe workplace.
3. Always be properly grounded when touching sensitive products, components, or assembly.
4. Store ESD-sensitive products in protective packaging or on antistatic mats.

2.2. Grounding Methods

To avoid electrostatic damage, observe the following grounding guidelines:

1. Cover workstations with approved antistatic material. Always wear a wrist strap connected to the workplace. Always use properly grounded tools and equipment.
2. Use antistatic mats, heel straps, or air ionizers for more protection.
3. Always handle electrostatically sensitive components by their edge or by their casing.
4. Avoid contact with pins, leads, or circuitry.
5. Switch off power and input signals before inserting and removing connectors or connecting test equipment.
6. Keep work area free of non-conductive materials such as ordinary plastic assembly aids and Styrofoam.
7. Use only field service tools that are conductive, such as cutters, screwdrivers, and vacuum cleaners.
8. Always place drives and boards PCB-assembly-side down on the foam.

2.3. Requirements IEC 62368-1

Users of the Q7ALx2 module must evaluate the end product to ensure the requirements of the IEC 62368-1 safety standard are met:

- The module must be installed in a suitable mechanical, electrical and fire enclosure.
- The module in its enclosure must be evaluated for temperature and airflow considerations.
- For interfaces having a power pin such as external power or fan, ensure that the connectors and wires are suitably rated.
- All connections from or to the Module shall be with Safety Extra Low Voltage (SELV) circuits only.
- Wires have suitable rating to withstand the maximum available power.
- The enclosure of any peripheral device fulfills the fire protecting requirements of IEC 62368-1.

2.4. Instructions for the Lithium Battery

The Q7ALx2 module is supported via a lithium battery on a separate carrier board. When replacing a lithium battery, only use the same or equivalent type or a replacement recommended by the manufacturer. Follow the replacement precautions stated below.

⚠CAUTION

Danger of explosion, when replaced with wrong type of battery. Replace only with the same or equivalent battery type recommended by the manufacturer. The lithium battery type must be UL recognized.

After removing the lithium battery, dispose of the lithium battery according to the regulations within your region.

Do not dispose of lithium batteries in general trash collection. Dispose of the battery according to the local regulations dealing with the disposal of these special materials, (e.g. to the collecting points for dispose of batteries).

3/ Scope of Delivery

3.1. Packing List

Check that your delivery is complete, and contains the item(s) below (according to the ordered configuration). If you discover damaged or missing item(s), contact your dealer.

Table 1: Packing List

Delivered Part	Part Description
Q7ALx2	Qseven® module board with Intel x86 SoC and on-module memory

Note: The above packing list is for standard single box package only.

3.2. Accessories

The following accessories are available for the Q7ALx2.

Table 2: Accessory List

Part Name	SAP Number	Part Description
Heatspreader Plate Commercial	81004-0000-99-1	Heatspeader to attach to commercial Qseven® Q7ALx2 module
Heatspreader Plate Industrial	81005-0000-99-1	Heatspeader to attach to industrial Qseven® Q7ALx2 module
Qseven-Eval Carrier	81100-000-00-0	Qseven® 2.1 pin-out Evaluation carrier board

4/ Description

The Qseven® Q7ALx2module is an off-the-shelf module designed to meet the Qseven® Specification Rev. 2.1.

The Q7ALx2 includes all the components of a common PC (Intel x86 SoC, on-module system memory, eMMC Flash memory expansion and extensive interfaces.) on a small form factor board (70 mm x 70 mm) designed for mounting on a carrier board using the Qseven® (MXM) connector. The carrier board powers the Q7ALx2 and the carrier board interfaces connect to the end application.

Figure 1: QSEVEN Module

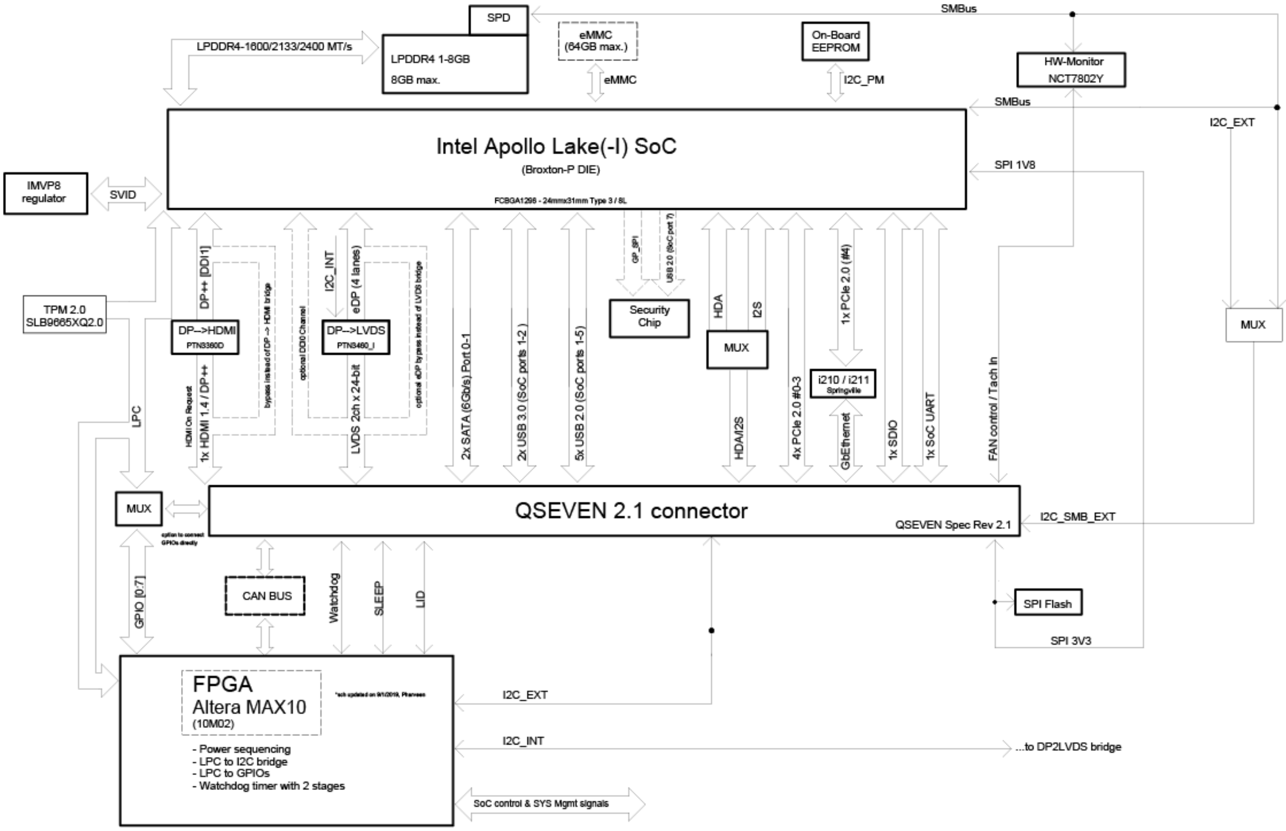
The main Qseven-Q7ALx2 features are:

- Intel® Atom x5 E3950, E3940, E3930 and mobile Celeron N3350/4200 with integrated chipset
- Qseven® form factor (70 mm x 70 mm)
- Qseven® connector complies to Qseven® specification Rev 2.1
- Up to 8 GByte LPDDR4 memory down
- From 32 GByte (pSLC) /up to 64 GB (MLC) eMMC 5.1 Flash (option)
- 2x SATA 6 Gb/s
- 4x PCIe x1, Gen 2
- 1x GbE LAN
- 2x USB 3.0 (QSEVEN port 0,1)
- 4x USB 2.0 Host (QSEVEN port 2, 3, 4, 5)
- 1x USB 2.0 OTG (QSEVEN port 1) using switch of full functional OTG
- 2x Display (1x eDP and 1x DP or HDMI)
- 1x SDIO
- 1x SPI external Boot (SPI0)
- 1x SPI for generic devices (SPI1)
- 1x HDA Audio / I2S Audio (muxed)
- 2x I2C interfaces
- 1x SMB interface
- 1x UART interfaces
- 8x GPIO's / LPC (muxed)
- 1x CAN Bus interface (option)

5/ Specification

5.1. Block Diagram

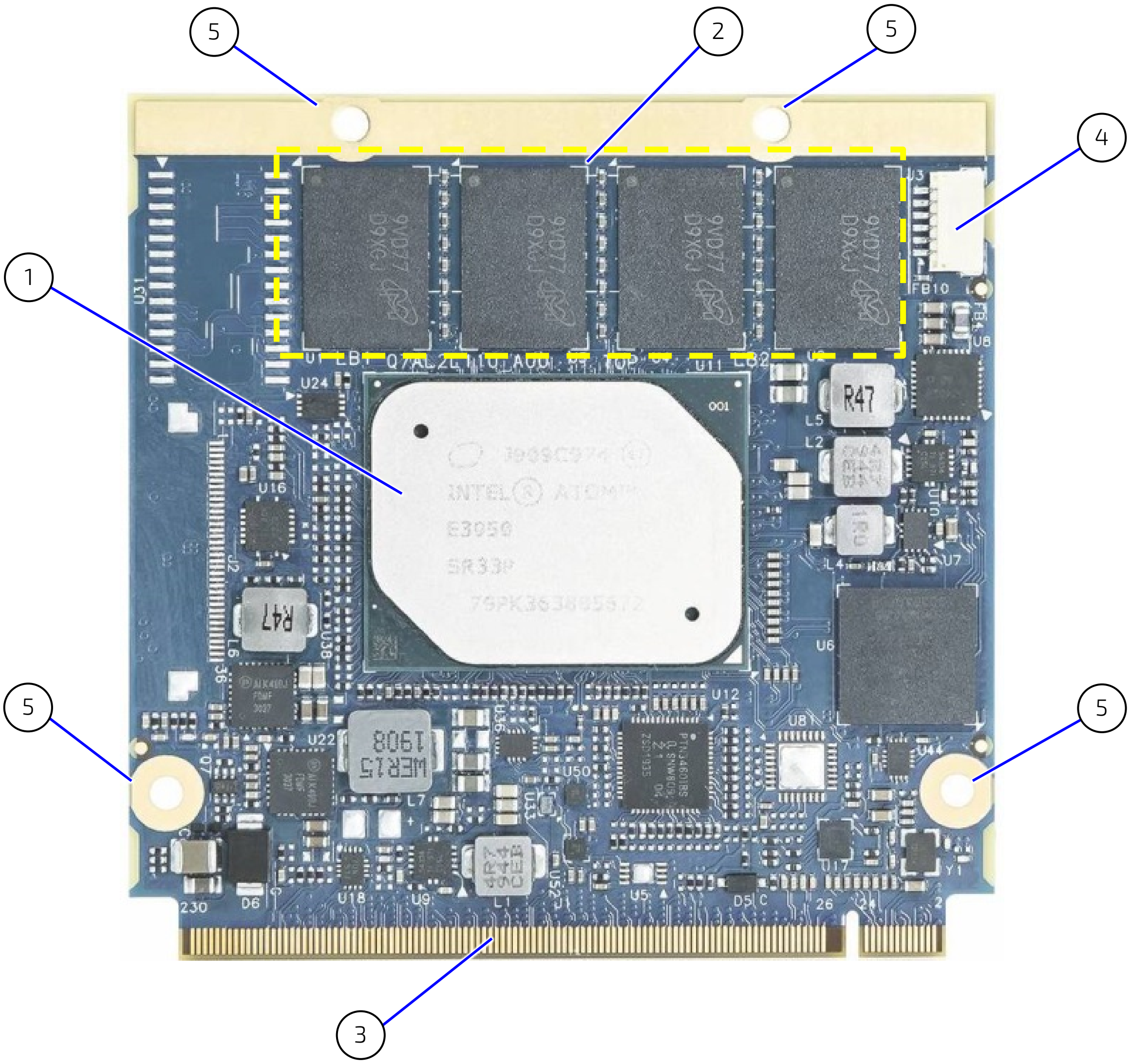
Figure 2 : Block Diagram Q7ALx2 Module



Note: Dashed outline is optional

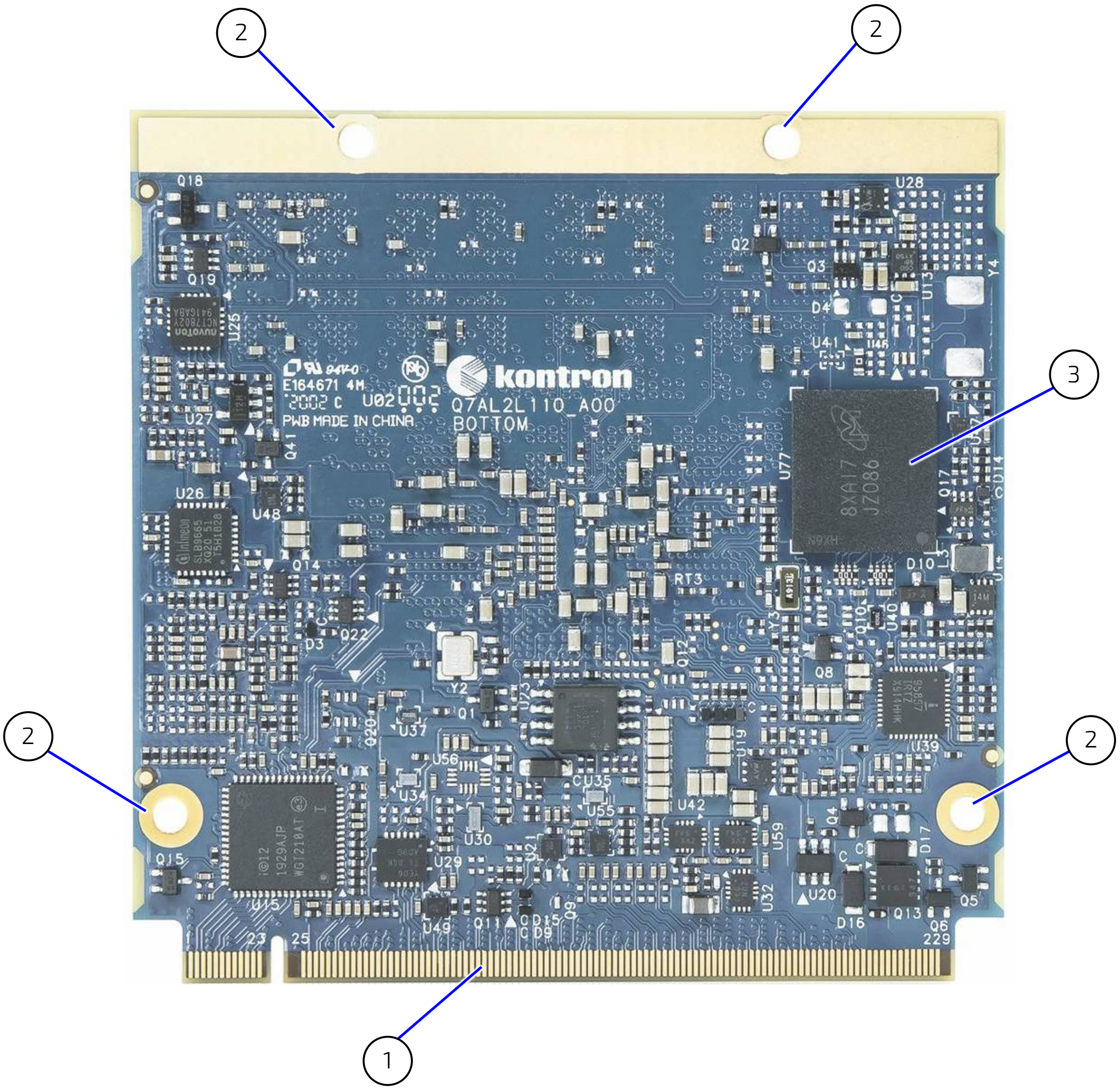
5.2. Module Views

Figure 3 : Top Side View Q7ALx2



1	SOC	4	CPLD connector
2	Memory down	5	4x Mounting points
3	Qseven® connector (top side)		

Figure 4 : Bottom Side View Q7ALx2



1	Qseven® connector (bottom side)	3	eMMC
2	4x Mounting points		

5.3. Component Technical Data

The table below summarizes the Q7ALx2 module's main component technical features:

Table 3: Component Technical Data

Q7ALx2 Module	
Form Factor	Qseven® module standardized form factor (70 mm x 70 mm)
Processor	
System On Chip (SOC)	Embedded processors based on Intel x86 SoC with integrated chipset: Industrial Grade (@ -40°C to 85°C): ▶ Intel Atom x5 E3930, 2 Cores, 1.8 GHz, 6,5 W ▶ Intel Atom x5 E3940, 4 Cores, 1.8 GHz, 9,5 W ▶ Intel Atom x7 E3950, 4 Cores, 2.0 GHz, 12 W Commercial Grade (0°C to 60°C): ▶ Intel Mobile Celeron N3350 2 Cores, 2.4 GHz, 6 W ▶ Intel Mobile Celeron N4200 2 Cores, 2.5 GHz, 6 W
Memory	
System Memory	▶ Up to 4x LPDDR4 1.2 V DRAMs ▶ Single channel ▶ Up to 8 GBytes (1 GB to 8 GB) ▶ 2400 MT/s
eMMC Storage (option)	▶ 2 GByte to 32 GByte (pSLC) eMMC 5.1 Flash or ▶ 2 GByte to 64 GByte (MLC) eMMC 5.1 Flash
Controller	
Embedded Controller	FPGA (MAX10) controller for embedded feature set and logic control
H/W Status Monitor	Nuvoton NCT7802Y hardware monitor supports: ▶ SM Bus connection to SoC ▶ PWM and Tach interface to external fan ▶ Temperature measurements (2x external thermal diodes and 1x internal sensor) ▶ Analog/Digital measurements on V_RTC, VCC and VCC_SB
Complex Programmable Logic Devices (CPLD)	CPLD (MAX10) controller supports: ▶ Power Sequencing ▶ Status and control signal level shifting to allow signals routed to Qseven® connector to comply with Qseven® Specifications ▶ LPC to UART bridge to provide 4-wire UART o (TX,RX,RTS,CTS) with FIFO legacy 16550 compliant ▶ LPC to I2C bridge to provide I2C interface ▶ LPC to GPIO bridge to provide eight GPIOs ▶ LPC to CAN bridge to provide CAN interface
Watchdog	Dual Staged Watchdog timer supported by: ▶ Watchdog time out (WDOUT) ▶ Watchdog trigger(WDTRIG#)

Software	
BIOS	On-board 128 Mb SPI flash for BIOS storage
Operating System Support	▶ Windows® 10 Enterprise 64 bit ▶ Windows 10 IoT 64 bit ▶ Linux Yocto 64-bit
I/O functions on Qseven® connector	
PCIe	4x PCIe Gen 2 (5 GT/s), lanes configured as: ▶ 4 x1 (4 PCIe links x 1 wide) ▶ 1 x4 (1 PCIe link x 4 wide) Note 1: Implement the PCIe links and support signals as per the Qseven® Specification. Note 2:The lane may not be configured as 2x2 Note 3: PCIe mapping is not supported in standard BIOS
SATA	2x SATA Gen 3 links (6Gb/s)
GbE LAN	1x GBE port (using Intel i210IT/i211AT Ethernet controller)
USB	2x USB 3.0 (USB 3.0 or USB 2.0 compatible)
	4x USB 2.0
	1x USB OTG (USB 2.0 host or client operation)
HDA	1x HDA audio (muxed with I2S interface)
I2S	1x Inter-IC Sound (I2S) interface (muxed with HDA interface)
Serial Port	1x 4-wire UART interface (TX, RX, CTS, RTS) at 3.3 VDC (supported by the MAX10 FPGA)
SPI	1x fast SPI interface from primary SPI chip for external boot from Carrier BIOS SPI chip 1x SPI interface as secondary SPI interface for generic SPI devices on the carrier board
CAN	1x CAN bus V2.0 interface (option)
I2C	2x I2C Interfaces (1x standard and 1x muxed with SMB)
GPIO	8x General Purpose Input/Output (GPIOs) configurable in BIOS (muxed with LPC bus)
SDIO	1x SDIO interface with the Qseven® connector
LVDS	Dual channel using eDP2LVDS or eDP + DP
On-module Connectors	
CPLD	1x CPLD,6-pin connector (used for JTAG)
Qseven®	1x Qseven® MXM, 230-pin connector (used for interfaces, control and power)
Power	
Power Supply	▶ VCC = 5 VDC +/- 5% ▶ VCC_SB = 5 VDC +/- 5% ▶ VCC_RTC = 3 VDC (Range: 2.4 VDC to 3.3 VDC)
Power Management	▶ Power saving supports C-states o C0, C1, C6, C7, C8, C9 and C10 ▶ Wake on LAN (WOL)
LID/SLeep/Batlow Signal	Supported

Display		
Digital Displays		Up to two independent digital displays using “DDI0” and “DDI1” from the SoC: ▶ DDI0 – eDP (no LVDS only shares Qseven® connector pin with LVDS) ▶ DDI1 - DP++ or HDMI
DDI0	eDP	eDP interface is DDI0 from SoC (Resolution: 3840x2160 @60Hz)
DDI1	HDMI	Dual Mode HDMI (Resolution: 3840x2160 @30Hz)
	DP++	DP++ interface is DDI1 from SoC (Resolution: 4096x2160 @60Hz)
Security		
TPM		TPM 2.0 (option)
Kontron Security Solution		Approtect supported (option)

5.4. Environmental Specification

Table 4: Environmental Specification

Environmental		
Temperature (operating)	Commercial grade	0°C to +60°
	Industrial grade (E2):	-40°C to +85°
Temperature (non-operating)	Commercial grade	-40°C to +85°C
	Industrial grade	
Relative Humidity	93%, at +40°C, non-condensing (according to IEC 60068-2-78)	
Vibration	According to IEC/EN60068-2-64	
Shock	According to IEC/EN60068-2-27	

5.5. Standards and Directives

The Qseven® Q7ALx2 module complies with the following Standards and Directives.

Table 5: Standards and Directives

CE			
National Certification		CE Marking Directive	93/68/EEC
		Low Voltage Directive (LVD)	2006/95/EC
EMC/EMI			
Emission	EN 55032 Class B	Test conducted in standard available chassis with Q7 carrier board. Electromagnetic compatible – Emission standard for information technology equipment (ITE). External test in certified test laboratory and declaration of conformity written by Kontron Technology only.	
Immunity	EN 61000-6-1	Test conducted in standard available chassis with Q7 carrier board. Electromagnetic compatible – Generic immunity standard Part1: Residential, commercial and light industrial environment. Internal test and declaration of conformity written by Kontron Technology only.	

Safety		
Europe	IEC 62368-1	Component recognition Audio/video, information and communication technology equipment – Safety requirements
USA & Canada	UL62368-1 CAN/CSA C22.2 No. 62368-1	
Environment		
WEEE	Compliant with the Waste Electrical and Electronic Equipment (WEEE) 2012/19/EU directive; to reduce waste of electrical and electronic equipment, encourage recycling and environmental disposal and increase the environmental awareness of producers	
RoHS II	Compliant with the Restriction of Hazardous Substances (RoHS) 2011/65/EU directive or the late status thereof, to reduce hazardous substances in electrical and electronic equipment	
REACH	Compliant with the Registration, Evaluation, Authorization and Restriction of Chemicals (REACH) Regulation No. 1907/2006 to identify the intrinsic properties of chemical substances earlier	

5.6. Mechanical Specification

Figure 5 : Q7ALx2 Top Side Mechanical Specification (measurement in mm)

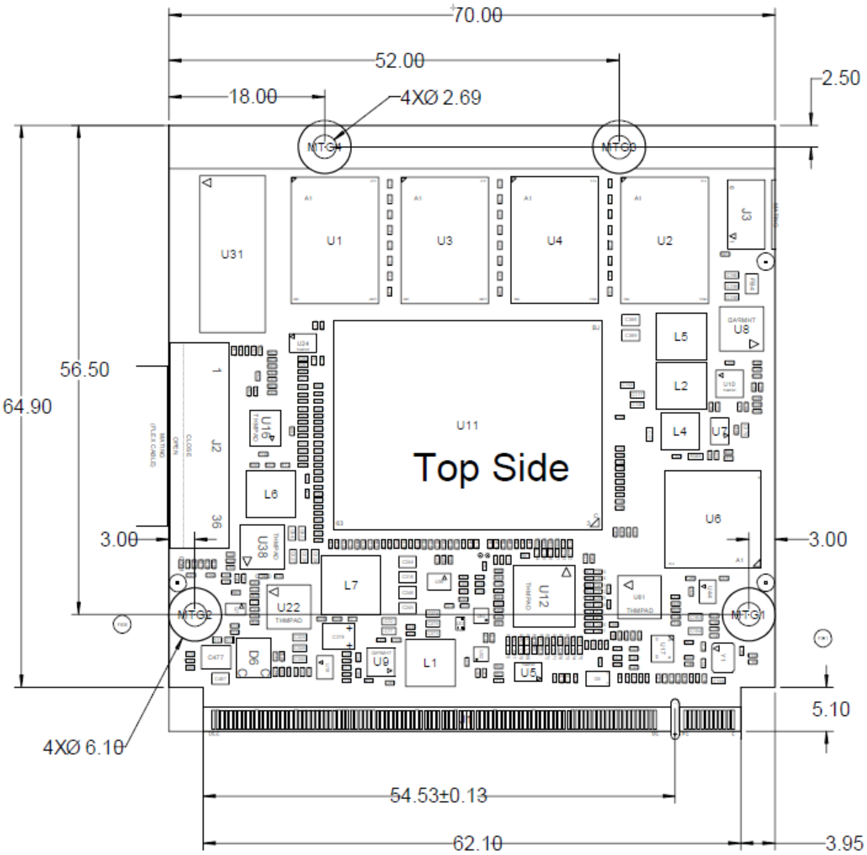
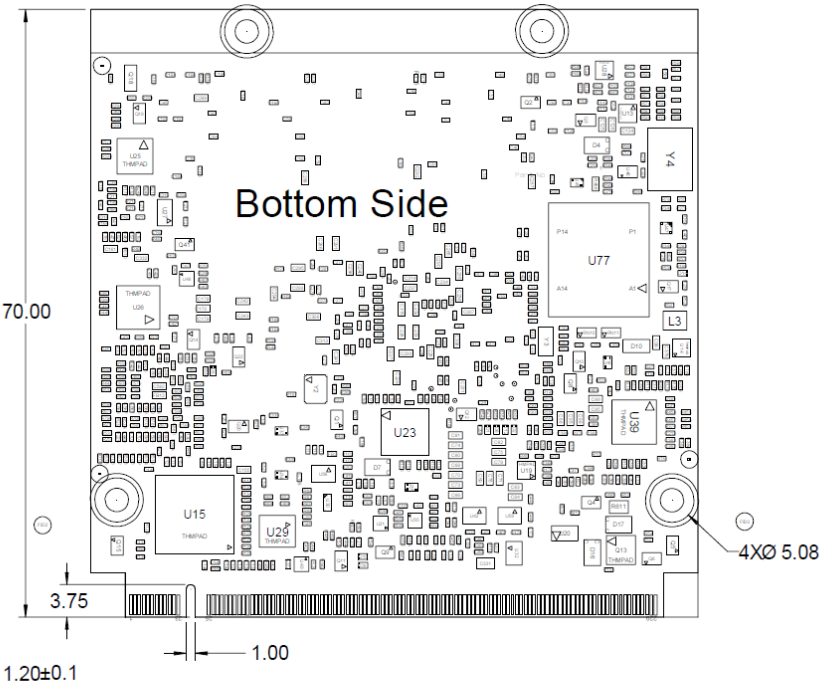


Figure 6: Q7ALx2 Bottom Side Mechanical Specification (measurement in mm)



5.6.1. Heat Spreader Mechanical Specification

Figure 7: Heat Spreader for Commercial Grade Mechanical Specification (measurement in mm)

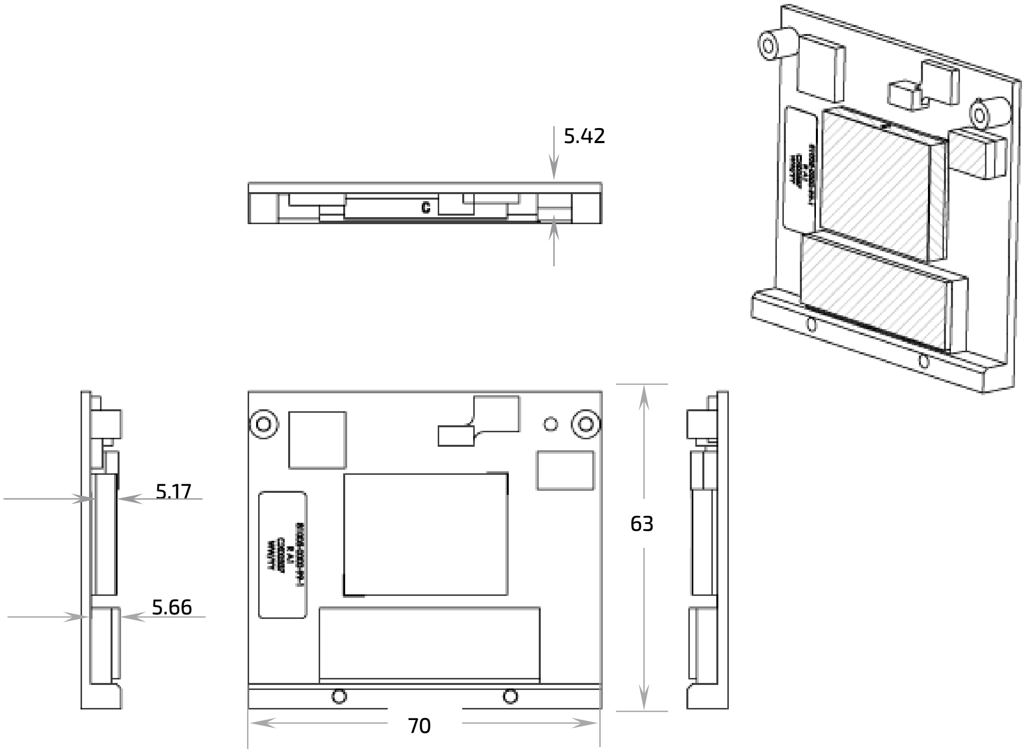
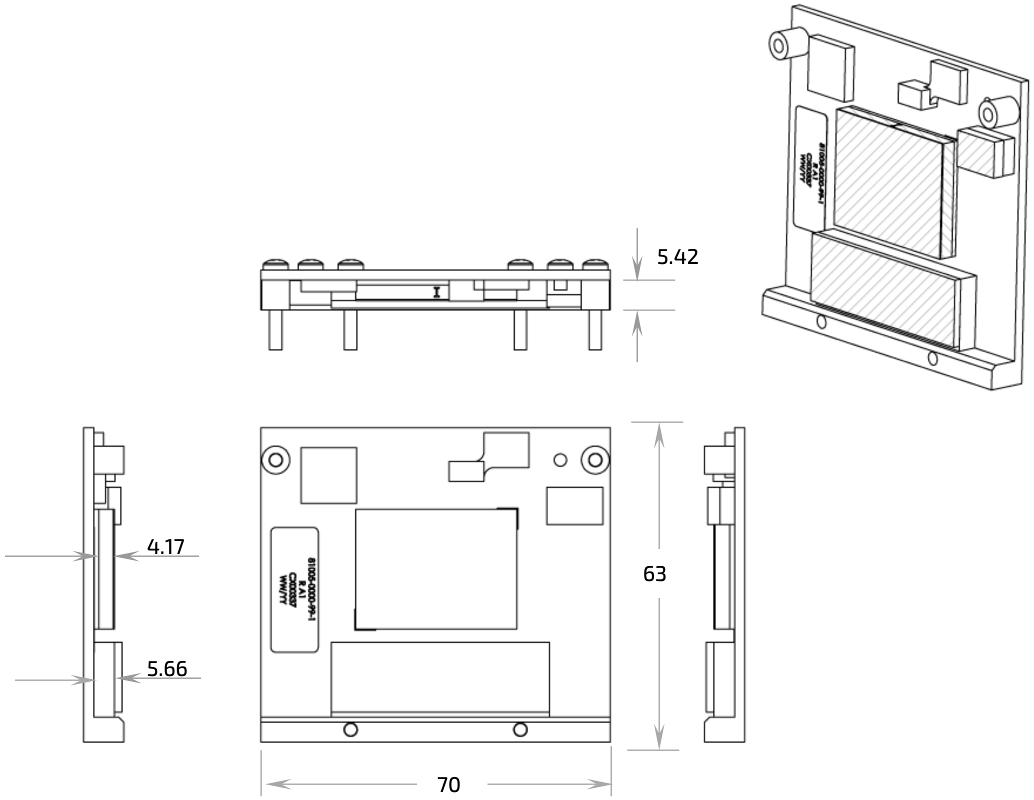


Figure 8: Heat Spreader for Industrial Grade Mechanical Specification (measurement in mm)



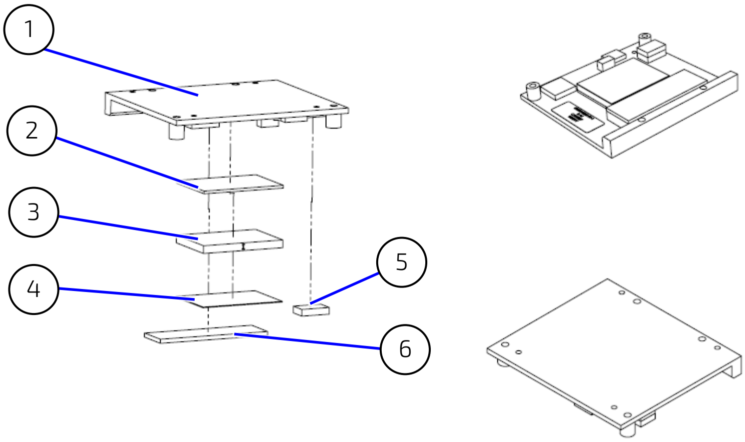
5.7. Thermal Management

5.7.1. Heatspreader Plate and Cooling Solutions

A heatspreader plate assembly is available for the Q7ALx2. The heatspreader plate is NOT a heat sink. The heatspreader plate is a Qseven® standard thermal interface to accompany a heat sink or external cooling device(s).

The aluminum slugs and thermal pads on the underside of the heatspreader plate act as thermal interfaces between the heatspreader plate and the major heat-generating components on the Q7ALx2 module. Approximately 80 % of the module's dissipated power is conducted to the heatspreader plate and can be removed by the cooling solution.

Figure 9: Heatspreader Plate Assembly



1	Heatspreader plate	4	Thermal pad
2	Thermal pad	5	Thermal pad
3	Aluminum slug	6	Thermal pad

An external cooling device must be used to maintain the heatspreader plate at the specified operating temperature. Under worst-case conditions, the cooling device must maintain an ambient air temperature and the heatspreader plate temperature, on any spot of the heatspreader's surface, must remain under the temperature grade's maximum specification of:

- 60°C for commercial grade modules
- 75°C for extended temperature grade modules
- 85°C for industrial temperature grade module

⚠CAUTION

Hot Surface

A Heatspreader plate or heatsink can get hot. To avoid burns and personal injury:

- Do not touch the when the product is operating
- Allow the product to cool before handling
- Wear protective gloves
- Switch off the product when not in use

⚠CAUTION

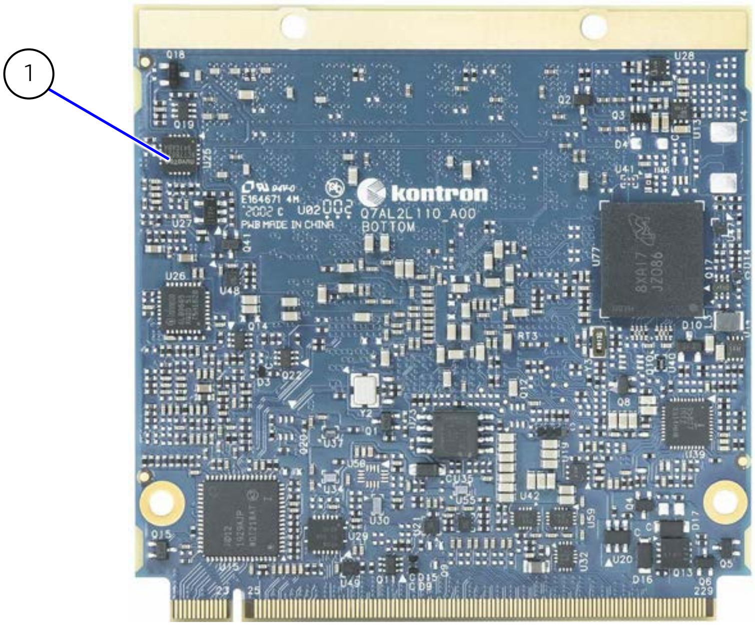
Operate only with an external cooling solution

To maintain the surface temperature of the heatspreader plate under the maximum temperature specified, an external cooling device such as a heatsink must be used.

5.7.2. Temperature Sensors

The Hardware Monitor (HWM) chip (Nuvoton NCT802Y) uses an on-chip temperature sensor to measure the module's temperature. This measurement is referred to as the "module temperature" in the BIOS setup menu (**Advanced>H/W Monitor**). The HWM uses the SMBus interface, see Table 13. SMBus Address.

Figure 10: HWM with Temperature Sensor



1 HWM Chip - measures "module temperature"

For documentation and CAD drawings of heatspreader plate and cooling solutions, refer to Kontron's Customer Section.

5.8. Power Specification

The Q7ALx2 module receives power from a carrier board via the Qseven® connector. The Q7ALx2 must be connected to a carrier board to power on.

⚠CAUTION

The Qseven® module is powered on by connecting to a carrier board using the Qseven® connector. Before connecting the module's Qseven® connector to the carrier board's corresponding connector, switched off and disconnected the carrier board from the main power supply. Failure to disconnect the main power supply could result in personal injury and damage to the module and/or carrier board.

5.8.1. Power Supply Specification

As defined by the Qseven® specification, the Q7ALx2 module is supplied with power using 5 VDC VCC pins on the Qseven® connector. A single +5 VDC input power rail drives the Q7ALx2 module. Additionally, two optional power rails supply other supported supply voltages such as +5 VDC standby and 3 VDC Real Time Clock (RTC). The RTC battery cell located on the carrier board provides the RTC voltage.

Table 6: Power Supply Specification

Supply Voltage (VCC)	5 VDC
Standby Voltage (VCC_SB)	5 VDC ±5 %
RTC Voltage (VCC_RTC)	3 VDC (Range: 2.4 VDC to 3.3 VDC)
Ground (GND)	Power Ground
Input Current	0.5 A per input voltage pin (max.)
Module Power	12W (when supplied with the minimum input voltage level (max.)

⚠CAUTION

Only connect the product to an external power supply providing the voltage type (AC or DC) and the input power (max. current) specified on the Kontron Product Label/within this user guide and meeting the requirements of the Limited Power Source (LPS) and Power Source (PS2) of UL/IEC 62368-1

5.8.2. Power Supply Voltage Rise Time

The input voltage rise time is 0.1 ms to 20 ms from input voltage ≤10% to nominal input voltage. To comply with the ATX specification there must be a smooth and continuous ramp up of each DC input voltage from 10 % to 90 % of the DC input voltage final set point.

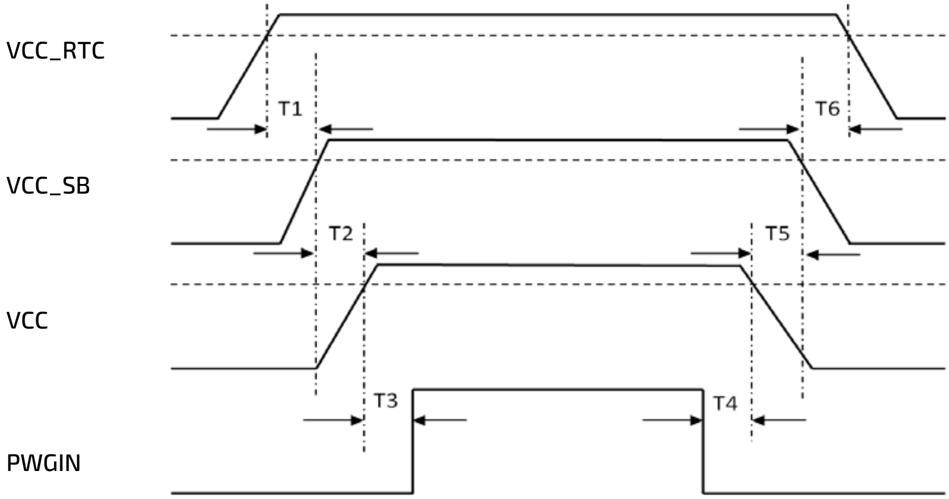
5.8.3. Power Supply Voltage Ripple

The maximum power supply voltage ripple for the input voltage range (+4.75 VDC to 5.25 VDC) is 50 mV peak-to-peak. The voltage ripple must not cause the input voltage range to be exceeded.

5.8.4. Input Power Sequencing

The following figure illustrates the Q7ALx2 module's inputs power start and stop sequence requirements.

Figure 11: Input Power Start and Stop Sequence



PWGIN is an active high input for the Qseven® module and indicate that the all the power rails on the carrier board are ready for use.

Start sequence

- VCC_RTC must come up at the same time or before VCC_SB comes up (T1)
- VCC_SB must come up at the same time or before VCC comes up (T2)
- PWGIN must be active at the same time or after VCC comes up (T3)

Stop Sequence

- PWGIN must be inactive at the same time or before VCC goes down (T4)
- VCC must go down at the same time or before VCC_SB goes down (T5)
- VCC_SB must go down at the same time or before VCC_RTC goes down (T6)

5.8.5. Power Management

Power management options are available within the BIOS setup. The Q7ALx2 implements the Advanced Configuration and Power Interface (ACPI) ACPI 3.0 hardware specification to control typical features such as power button and suspend states.

If power is removed, 5 VDC can be applied to VCC_SB pins (pins 205 and 206) to support the suspend-states:

- Suspend-to-Disk (S4)
- Soft-off state (S5)

Implementing the wake-up event (S0) requires a connection to power, as the module will be started.

5.8.5.1. Power Supply Control and Management Signals

Power supply control settings are set in the BIOS setup menus and enable the module to shut down, rest and wake from standby.

Table 7: Power Supply Control and Management Signals

Signal	Pin	Description	I/O Type	IOL/ IIL	I/ O
PWRBTN#	20	Power button: this signal is a low active input and triggered on the falling edge	CMOS 3.3V Standby	≥ 10 mA	I
PWGIN#	26	Power good input: this high active input for the Qseven® module indicates that all power rails located on the carrier board are ready for use.	CMOS 5V	≥ 4 mA	I
RSTBTN#	28	Reset button: this input may be driven active low by external circuitry to reset the Qseven® module.	CMOS 3.3V	≥ 10 mA	I
BATLOW#	27	Battery low: this signal may be driven active low by external circuitry to signal that the system battery is low or may be used to signal some other external battery management event.	CMOS 3.3V Suspend	≥ 10 mA	I
Wake#	17	Wake Event: this may be driven active low by external circuitry to signal an external wake-up event.	CMOS 3.3V Suspend	≥ 10 mA	I
SUS_S3#	18	S3 State: this signal shuts off power to all runtime system components that are not maintained during S3 (Suspend to Ram), S4 or S5 states. The signal SUS_S3# is necessary in order to support the optional S3 cold power state.	CMOS 3.3V Suspend	≥ 1 mA	O
SUS_S5#	16	S5 State: This signal indicates S4 or S5 (Soft Off) state.	CMOS 3.3V Suspend	≥ 1 mA	O
SLP_BTN#	21	Sleep button: this low active signal transitions the module into the sleep state or to wake up the system up. This signal is triggered on falling edge. (Pin shared with GPIO)	CMOS 3.3V Suspend	≥ 10 mA	I
LID_BTN#	22	LID button: this low active signal detects a LID switch and brings the module into the sleep state or wakes up the module again. Open/Close state may be software configurable. (Pin shared with GPIO)	CMOS 3.3V Suspend	≥ 10 mA	I

The SUS_S3# signal must be able to enable the carrier board's power rails generated out of the VCC power rail.

6/ Features and Interfaces

6.1. CAN Bus

The CAN Bus interface is compliant with the CAN Bus V 2.0 specification and implemented via a LPC to GPIO bridge. In order to connect a CAN controller device to the Qseven ® module's CAN bus it is necessary to add transceiver hardware to the carrier board.

6.2. eMMC (option)

The Embedded Multimedia Flash Card (eMMC) is eMMC 5.1 compatible and supports eMMC flash capacities from 2 GByte to 32 GByte (pSLC) or from 2 GByte to 64 GByte (MLC). During the manufacturing process, Multi Level Cell (MLC) eMMC is reconfigured to act as pseudo Single Level Cell (pSLC) eMMC to provide improved reliability, endurance and performance.

The eMMC flash memory features are:

- Up to 32 GByte (pSLC) / 64 GB (MLC) eMMC 5.1 Flash
- eMMC 5.1 compatible

6.3. Debug Port - JTAG

The Joint Test Action Group (JTAG) is an industry standard used to verify designs and test modules or boards after they have been manufactured. JTAG tests for common problems by observing data at the device's inputs and controlling the data at the outputs. Simple tests can be performed to find manufacturing defects such as missing devices unconnected pins or failed/dead devices. The JTAG signals are: TDI (Test Data In), TDO (Test Data Out), TMS (Test Mode Select), TCK (Test Clock), and TRST (Test Report-optional).

6.4. Fast I2C

Fast I2C (100 to 400 kHz) supports transfer between components on the same board. The Qseven-Q7ALx2 features two I2C Interfaces. One standard I2C interface and one I2C interface multiplexed with the SM Bus.

The I2C controller supports:

- Multimaster transfers
- Clock stretching
- Collision detection
- Interruption on completion of an operation

6.5. GPIO

The eight GPIO pins GPI00 (pin 185), GPIO1 (pin 186), GPIO2 (pin 187), GPIO3 (pin 188), GPIO4 (pin 189), GPIO5 (pin 190), GPIO6 (pin 191) and GPIO7 (pin 192) on the Qseven® connector are pin shared with the LPC. An EEPROM bit is added so that the carrier board can define if the pins are used as GPIO or LPC.

The GPIO or LPC option is configured in the BIOS setup:

Advanced>CPLD Configuration>GPIO-LPC Mux Select [Mux to LPC, Mux to GPIO]

6.6. Kontron Security Solution (option)

The Kontron security solution is a combined hardware and software solution that includes an embedded hardware security module and a software framework to protect applications.

The integrated security module connected to SoC port 7. Therefore, if this option is installed, SoC port 7 is not available for other interfaces. The main integrate security solution features are:

- Copy protection
- IP protection
- License model enforcement

If required, customers can customize the solution to meet specific needs. For more information, contact Kontron Support.

6.7. LPC

The Low Pin Count (LPC) interface signals are connected to the LPC bus bridge located in the CPU or integrated chipset. The LPC low speed interface can be used for peripheral circuits such as an external Super I/O controller that typically combines legacy-device support into a single IC. The implementation of this sub-system complies with the Qseven® Specification.

The LPC bus does not support DMA (Direct Memory Access). When more than one device is used on LPC, a zero delay clock buffer is required that can lead to limitations for the ISA bus.

The LPC Interface signals LPC_AD0 (pin 185), LPC_AD1 (pin 186), LPC_AD2 (pin 187), LPC_AD3 (pin 188), LPC_CLK (pin 189), LPC_FRAME# (pin 190) and LPC_LDRQ# (pin 192) on the Qseven® connector are pin shared with the GPIO. The CPLD controller incorporates a LPC bridge to support either I2C, to GPIO. An EEPROM bit on the carrier board can define if the pins are used as GPIO or LPC.

The GPIO or LPC option is configured in the BIOS setup:

Advanced>CPLD Configuration>GPIO-LPC Mux Select [Mux to LPC, Mux to GPIO]

Table 8: Supported BIOS Features

LPC	Interface Signals	Description
LPC Bridge to	UART	4-wire UART
	GPIO	8x GPIOs
	CAN	Used GPIO bridge to support CAN interface
	I2C	I2C interface
	PS/2	Not supported
	LPT	Not suppored
	Floppy	Not supported

Interface signal marked as not supported (PS/2, LPT and Floppy) do not exclude OS support (e.g. Hardware Monitor (HWM) is accessible via SMB). If any other LPC Super I/O additional BIOS implementations are necessary, contact Kontron Support.

6.8. RTC

The Real Time Clock (RTC) keeps track of the current time accuratly. The RTC's low power consumption means that the RTC can be powered from an alternative source of power, enabling the RTC to continue to keep time while the primary source of power is off or unavailable. The Q7ALx2 module's RTC battery voltage range is 2.4 V - 3.3 V.

6.9. SDIO

The Secure Digital Input/Output (SDIO) interface is used to interchange data between devices. Using an SDIO card, data can be interchanged between portable or non-portable memory. The 4-bit SDIO transmits data on SDIO_DAT1 (pin 148), SDIO_DAT1 (pin 149), SDIO_DAT3 (pin 149) and SDIO_DAT4 (pin 150) and controls the data using pins 142, 143, 145, 146 and 147 on the Qseven® connector.

6.10. SPI

The Serial Peripheral Interface Bus (SPI) bus is a synchronous four-wire serial data link standard. Devices communicate in master/slave mode, where the master device initiates the data frame. .A master device can control one or multiple slave device(s) by setting the slave's (chip select) line.

The Q7ALx2 module supports one SPI interface. The SPI interface is connected to the primary SPI chip on the module and can also be used to boot from the external BIOS SPI chip on the carrier board.

i **The SPI interface can boot from the primary on-module SPI chip or with an external SPI BIOS chip on the carrier board.**

6.10.1. SPI boot

SPI boot is perfomed from the module's 128 Mb SPI Flash used for BIOS storage or the carrier board's Flash pin (Module_BIOS_DIS#).

Table 9: SPI Boot Pin Configuration

Configuration	MODULE_BIOS_DIS#	Function
1	Open	Boot on module BIOS
2	GND	Boot on carrier board BIOS

i **The BIOS does not support being split between two chips. Booting takes place either from the module SPI or from the carrier board SPI.**

SPI boot is available for multiple vendors. The following table lists the supported SPI Boot Flash types for the 8-SOIC package.

Table 10: Supported SPI Boot Flash Types for 8-SOIC Package

Size	Manufacturer	Part Number	Device ID
16MB	Maxim	MX25L12835F	0x20
16MB	Winbond	W25Q128	0x90
16MB	Micron	N25Q128A	0xBA

6.11. SpeedStep™ Technology

The SpeedStep™ technology enables the adaption of high performance computing in applications by switching automatically between maximum performance mode and battery-optimized mode, depending on the needs of the application. When battery powered is running in idle mode, the processor drops to lower frequencies (by changing the CPU ratios) and voltage, thus conserving battery life while maintaining a high level of performance. The frequency is automatically set back to the higher 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 setup, manual control or modification of the CPU performance is possible. To achieve manual control, setup the CPU Performance States (P-state and C-state), use third party software to control the CPU Performance States.

6.12. TPM 2.0 (option)

The Trusted Platform Module (TPM) stores RSA encryption keys specific to the host system for hardware authentication. The term TPM refers to the set of specifications applicable to TPM chips. The LPC bus connects the TPM chip to the CPU.

Each TPM chip contains an RSA key pair called the Endorsement Key (EK). The pair is maintained inside the TPM chip and cannot be accessed by software. The Storage Root Key (SRK) is created when a user or administrator takes ownership of the system. This key pair is generated by the TPM based on the Endorsement Key and an owner-specified password.

A second key, called an Attestation Identity Key (AIK) protects the device against unauthorized firmware and software modification by hashing critical sections of firmware and software before they are executed. When the system attempts to connect to the network, the hashes are sent to a server that verifies they match the expected values. If any of the hashed components have been modified since the last start, the match fails, and the system cannot gain entry to the network.

To use TPM, the TPM feature must be enabled in the BIOS setup. To enable the TPM feature in the BIOS setup:

Advanced>Trusted Computing>Security Device> [Enable, Disable]

Select the TPM version or allow for auto select in the BIOS setup:

Advanced>Trusted Computing>Device Select> [TPM 1.2, TPM2.0, AUTO]

6.13. UART

The 4-wire UART supported by MAX10 FPGA implements a serial communication interface (COM) and supports one serial RX/TX port on the Qseven® connector's pin-171 (UART0_TX) and pin-177 (UART0_RX) for UART0. The UART controller is fully 16550A compatible.

UART features are:

- On-Chip bit rate (baud rate) generator
- With handshake lines
- Interrupt function to the host
- FIFO buffer for incoming and outgoing data

6.14. Watchdog Timer (WDT) - Dual Stage

A watchdog timer (WDT) or (computer operating properly (COP) timer) is a computer hardware or software timer. If there is a fault condition in the main program, the watchdog triggers a system reset or other corrective actions. The intention is to bring the system back from the non-responsive state to normal operation.

Possible fault conditions are a hang, or neglecting to service the watchdog regularly. Such as writing a “service pulse” to it, also referred to as “kicking the dog”, “petting the dog”, “feeding the watchdog” or “triggering the watchdog”.

The Q7ALx2 module offers a watchdog that works with two stages that can be programmed independently and used stage by stage.

Table 11: Dual Staged Watchdog Timer- Time-Out Events

0000b	No action	Stage is off and will be skipped.
0001b	Reset	A reset restarts the module and starts a new POST and operating system.
0101b	Delay -> No action	Might be necessary when an operating system must be started and the time for the first trigger pulse must be extended. Only available in the first stage.
1000b	WDT Only	This setting triggers the WDT pin on the QSEVEN® connector (pin 72) only.
1001b	Reset + WDT	
1010b	NMI + WDT	
1011b	SMI + WDT	
1100b	SCI + WDT	
1101b	DELAY + WDT -> No action	

6.14.1. Watchdog Timer Signal

Watchdog time-out event (pin-72) on the Qseven® connector provides a signal that can be asserted when a watchdog timer has not been triggered within a set time. The WDT signal is configurable to any of the two stages. After reset, the signal is automatically de-asserted. If de-assertion is necessary during runtime, contact Kontron Support for further help.

7/ System Resources

7.1. PCI Devices

All devices follow the Peripheral Component Interconnect (PCI) 2.3 and PCI Express Base 1.0a specification. The BIOS and Operating System (OS) control the memory and I/O resources. For more information, refer to the PCI 2.3 Specification.

7.2. I2C Bus

The 8-bit I2C address uses the Least Significant Bit (LSB) of the binary address to indicate whether the address is a read or write address:

- LSB = 0 defines a write
- LSB = 1 defines a read

The following table specifies the devices connected the I2C bus with I2C address.

Table 12: I2C Bus Port Address

8-bit Address	7-bit Address	Device	Comment
A0h	50h	Module EEprom	Stores Module Information and uses 12C to interface with the carrier board
C0h	60h	PTN3460	eDP to LVDS bridge

7.3. SM Bus

The System Management (SM) Bus is an 8-bit address bus where the LSB (Bit 0) defines the direction (read/write).

- Bit 0 = 0 defines the write address
- Bit 0 = 1 defines the read address

The hexadecimal 8-bit addresses listed below show the write address for all devices. The hexadecimal 7-bit SMBus addresses show the device address without bit0.

Table 13. SMBus Address

8-bit Address	7-bit Address	Device	Comment
5Ch	2Eh	HWM NCT7802Y	Do not use under any circumstances
A0h	50h	LPDDR4 DRAM0 SPD	Memory down on the module, 4x LPDDR4, channel 1

8/ Connectors

8.1. Signal Terms

The terms used to describe the Qseven® module's connectors signals are:

Table 14: Qseven® Signal Terms

Term	Description	Comment
I	Input Pin	
O	Output Pin	
OC	Open Collector	
OD	Open Drain	
PP	Push Pull	
I/O	Input/Output Pin	Bi-directional data flow
IOL	Output low current	Maximum output low current the module must be able to drive to an external circuitry.
IIL	Input low current	Maximum input low current that must be provided to the module (via external circuitry) to guarantee a proper logic low level of the signal.
CMOS	Logic input or output.	
CMOS OD	Open Drain Logic input or output	
D-PHY	Display.PHY	A serial interface using differential signaling for band- limited channels with scalable data lanes and a source synchronous clock to support power efficient interfaces for streaming applications such as displays and cameras.
NC	Not Connected	
	Reserved	No available for the user

8.2. Qseven® MXM 230 Pin Assignment

The Qseven® connector is MXM 230-pin connector with the same number of pins on the top and bottom sides.

All required PU or PD resistors are implemented on the Qseven® module. This ensures that signals that are not used will be left floating. Termination of all signals will always be on the module unless otherwise stated.

Table 15: QSEVEN® Module Connector Pin Assignment of Bottom Side

Pin	Signal Row (bottom side)	Description	I/O Type	Termin-ation	IOL/ IIL	I/O
1	GND	Power Ground	Power			
3	GBE_MDI3-	Media Dependent Interface (MDI) differential pair 3	GB_LAN			I/O
5	GBE_MDI3+	Media Dependent Interface (MDI) differential pair 3	GB_LAN			I/O
7	GBE_LINK100#	Ethernet controller 0 100Mbit/sec link indicator, active low.	CMOS 3.3V PP		Max. 10 mA	O
9	GBE_MDI1-	Media Dependent Interface (MDI) differential pair 1 1	GB_LAN			I/O
11	GBE_MDI1+	Media Dependent Interface (MDI) differential pair 1 1	GB_LAN			I/O
13	GBE_LINK#	Ethernet controller 0 link indicator, active low.	CMOS 3.3V PP		Max. 10 mA	O
15	GBE_CTREF		REF			
17	WAKE#	External system wake event. This may be driven active low by external circuitry to signal an external wake-up event.	CMOS 3.3V Suspend	PU 10 kΩ 3.3V S5	≥10 mA	I
19	GPO0	General Purpose Output 0	CMOS 3.3V	PD/PU In CPU		O
21	SLP_BTN# / GPII1	Sleep button. Low active signal used by the ACPI operating system to transition the system into sleep state or to wake it up again. (falling edge triggered) / Optionally interrupt-capable General Purpose Input 1	CMOS 3.3V Suspend CMOS 3.3V	PU 10 kΩ 3.3V S5	≥10 mA	I
23	GND	Power Ground	Power			
KEY						
25	GND	Power Ground	Power			
27	BATLOW# / GPII2	Battery low input may be driven active low by external circuitry indicating system battery is low or to signal an external battery management event. Optionally interrupt-capable General Purpose Input 2	CMOS 3.3V Suspend CMOS 3.3V	PU 10 kΩ 3.3V S5	≥10 mA	I
29	SATA0_TX+	SATA channel 0, Transmit Input differential pair	SATA			O
31	SATA0_TX-	SATA channel 0, Transmit Input differential pair	SATA			O
33	SATA_ACT#	SATA Led. Open collector output pin driven during SATA command activity.	OC 3.3 V	PU 10 kΩ 3.3V S0	Max. 10 mA	O
35	SATA0_RX+	SATA channel 0, Receive Input differential pair	SATA			I
37	SATA0_RX-	SATA channel 0, Receive Input differential pair	SATA			I
39	GND	Power Ground	Power			
41	BIOS_DISABLE# / BOOT_ALT#	Reserved (optional on the carrier)				
43	SDIO_CD#	SDIO Card Detect. indicates a SDIO/MMC card is present.	CMOS 3.3V	PU 10 kΩ 3.3V S5		I/O
45	SDIO_CMD	SDIO Command/Response for card initialization (Open Drain) and command transfers (Push Pull)	CMOS 3.3V OD/PP			I/O

Pin	Signal Row (bottom side)	Description	I/O Type	Termin-ation	IOL/ IIL	I/O
47	SDIO_PWR#	SDIO Power Enable to power a SD/MMC card device	CMOS 3.3V			O
49	SDIO_DAT0	SDIO Data lines operate in push-pull mode.	CMOS 3.3V PP			I/O
51	SDIO_DAT2	SDIO Data lines operate in push-pull mode.	CMOS 3.3V PP			I/O
53	Reserved					
55	Reserved					
57	GND	Power Ground	Power			
59	HDA_SYNC / I2S_WS	Serial Bus Synchronization Multiplexed with I2S Word Select from Codec	CMOS 3.3V			O
61	HDA_RST# / I2S_RST#	HD Audio Codec Reset Multiplexed with I2S Codec Reset	CMOS 3.3V			O
63	HDA_BITCLK / I2S_CLK	HD Audio 24 MHz Serial Bit Clock from Codec Multiplexed with I2S Serial Data Clock from Codec	CMOS 3.3V			O
65	HDA_SDI / I2S_SDI	HD Audio Serial Data Input from Codec. Multiplexed with I2S Serial Data Input from Codec	CMOS 3.3V			I
67	HDA_SDO / I2S_SDO	HD Audio Serial Data Output to Codec Multiplexed with I2S Serial Data Output from Codec.	CMOS 3.3V			O
69	THRM#	Active Low -Thermal Alarm generated by external hardware indicates over temperature and initiate thermal throttling.	CMOS 3.3V	PU 10 kΩ 3.3V S0		I
71	THRMTRIP#	Active Thermal Trip indicates processor overheating and immediate transitions to S5 State (Soft Off).	CMOS 3.3V	PU 10 kΩ 3.3V S0		O
73	GND	Power Ground	Power			
75	USB_P7- / USB_SSTX0-	Universal Serial Bus Port 7 differential pair / USB Superspeed receive signal differential pair 0	USB			I/O I
77	USB_P7+ / USB_SSTX0+	Universal Serial Bus Port 7 differential pair / USB Superspeed transmit signal differential pair 0	USB			I/O O
79	USB_6_7_OC#	Monitors the USB power over current of the USB Ports 6 & 7	3.3V Suspend	PU 10 kΩ 3.3V S5	≥5 mA	I
81	USB_P5- / USB_SSTX2-	Universal Serial Bus Port 5 differential pair / USB Superspeed transmit signal differential pair 2	USB			I/O O
85	USB_2_3_OC#	Monitors the USB power over current of the USB Ports 2 & 3	3.3V Suspend	PU 10 kΩ 3.3V S5	≥5 mA	I
87	USB_P3-	Universal Serial Bus Port 3 differential pair	USB			I/O
89	USB_P3+	Universal Serial Bus Port 3 differential pair	USB			I/O
91	USB_VBUS	USB VBUS pin, 5V tolerant. VBUS resistance placed on module and capacitance on carrier board.	CMOS 5.0V		<=2.5mA B-device	I
93	USB_P1-	Universal Serial Bus Port 1 differential pair	USB			I/O
95	USB_P1+	Universal Serial Bus Port 1 differential pair	USB			I/O
97	GND	Power Ground	Power			
99	eDP0_TX0+ / LVDS_A0+	embedded DP primary channel differential pair 0/ LVDS primary channel differential pair 0	eDP/DP / LVDS			O O
101	eDP0_TX0- / LVDS_A0-	embedded DP primary channel differential pair 0/ LVDS primary channel differential pair 0	eDP/DP / LVDS			O
103	eDP0_TX1+ / LVDS_A1+	embedded DP primary channel differential pair 1/ LVDS primary channel differential pair 1	eDP/DP / LVDS			O
105	eDP0_TX1- / LVDS_A1-	embedded DP primary channel differential pair 1/ LVDS primary channel differential pair 1	eDP/DP / LVDS			O

Pin	Signal Row (bottom side)	Description	I/O Type	Termin-ation	IOL/ IIL	I/O
107	eDP0_TX2+ / LVDS_A2+	embedded DP primary channel differential pair 2/ LVDS primary channel differential pair 2	eDP/DP / LVDS			O
109	eDP0_TX2- / LVDS_A2-	embedded DP primary channel differential pair 2/ LVDS primary channel differential pair 3	eDP/DP / LVDS			O
111	LVDS_PPEN	Controls the panel power enable	CMOS 3.3V		Max. 1 mA	O
113	eDP0_TX3+ / LVDS_A3+	embedded DP primary channel differential pair 3/ LVDS primary channel differential pair 3	eDP/DP / LVDS			O
115	eDP0_TX3- / LVDS_A3-	embedded DP primary channel differential pair 3/ LVDS primary channel differential pair 3	eDP/DP / LVDS			O
117	GND	Power Ground	Power			
119	eDP0_AUX+ / LVDS_A_CLK+	embedded DP primary auxiliary channel/ LVDS primary channel differential pair clock line	eDP/DP / LVDS			O
121	eDP0_AUX- / LVDS_A_CLK-	embedded DisplayPort primary auxiliary channel/ LVDS primary channel differential pair clock line	eDP/DP / LVDS			O
123	LVDS_BLT_CTRL / GP_PWM_OUT0	Primary functionality is to control the panel backlight brightness via pulse width modulation (PWM). Or can be used as General Purpose PWM Output.	CMOS 3.3V			O
125	LVDS_DID_DAT / GP2_I2C_DAT	Primary functionality DisplayID DDC data line used for LVDS flat panel detection. Or can be used as a General Purpose I2C bus #2 data line.	CMOS 3.3V OD /	PU 10 kΩ 3.3V S0		I/O
127	LVDS_DID_CLK / GP2_I2C_CLK	Primary functionality is DisplayID DDC clock line used for LVDS flat panel detection. Or can be used as a General Purpose I²C bus #2 clock line.	CMOS 3.3V OD/	PU 10 kΩ 3.3V S0		I/O
129	CAN0_TX	Output for CAN Bus channel 0. To connect a CAN controller device to module's CAN bus it is necessary to add transceiver hardware to the carrier board.	CMOS 3.3V			O
131	DP_LANE3+ / TMDS_CLK+	DisplayPort differential pair lines lane 3. Or TMDS differential pair clock lines.	eDP/DP / TMDS			O
133	DP_LANE3- / TMDS_CLK-	DisplayPort differential pair lines lane 3. Or TMDS differential pair clock lines.	eDP/DP / TDMS			O
135	GND	Power Ground	Power			
137	DP_LANE1+ / TMDS_LANE1+	DisplayPort differential pair lines lane 1 Or TMDS differential pair lines lane 1	eDP/DP / TDMS			O
139	DP_LANE1- / TMDS_LANE1-	DisplayPort differential pair lines lane 1 Or TMDS differential pair lines lane 1	eDP/DP / TDMS			O
141	GND	Power Ground	Power			
143	DP_LANE2+ / TMDS_LANE0+	DisplayPort differential pair lines lane 2 Or TMDS differential pair lines lane 0	eDP/DP / TDMS			O
145	DP_LANE2- / TMDS_LANE0-	DisplayPort differential pair lines lane 2 Or TMDS differential pair lines lane 0	eDP/DP / TDMS			O
147	GND	Power Ground	Power			
149	DP_LANE0+ / TMDS_LANE2+	DisplayPort differential pair lines lane 0 Or TMDS differential pair lines lane 2	eDP/DP / TDMS			O
151	DP_LANE0- TMDS_LANE2-	DisplayPort differential pair lines lane 0 **Or** TMDS differential pair lines lane 2	eDP/DP / TDMS			O
153	HDMI_HPD#	Hot plug detection signal that serves as an interrupt request.	CMOS 3.3V	PU 100kΩ 3.3V S0		I
155	PCIE_CLK_REF+	PCI Express Reference Clock for Lanes 0 to 3.	PCIe			O

Pin	Signal Row (bottom side)	Description	I/O Type	Termin-ation	IOL/ IIL	I/O
157	PCIE_CLK_REF-	PCI Express Reference Clock for Lanes 0 to 3.	PCIe			O
159	GND	Power Ground	Power			
161	PCIE3_TX+	PCIe channel 3, Transmit Input differential pair.	PCIe			O
163	PCIE3_TX-	PCIe channel 3, Transmit Input differential pair.	PCIe			O
165	GND	Power ground	Power			
167	PCIE2_TX+	PCIe channel 2, Transmit Input differential pair.	PCIe			O
169	PCIE2_TX-	PCIe channel 2, Transmit Input differential pair.	PCIe			O
171	UART0_TX	Serial Data Transmitter	CMOS 3.3V		Max. 1 mA	O
173	PCIE1_TX+	PCIe channel 1, Transmit Input differential pair.	PCIe			O
175	PCIE1_TX-	PCIe channel 1, Transmit Input differential pair.	PCIe			O
177	UART0_RX	Serial Data Receiver	CMOS 3.3V		≥5mA	I
179	PCIE0_TX+	PCIe channel 0, Transmit Input differential pair.	PCIe			O
181	PCIE0_TX-	PCIe channel 0, Transmit Input differential pair.	PCIe			O
183	GND	Power Ground	Power			
185	LPC_AD0 / GPIO0	Multiplexed Command, Address and Data/ General purpose input/output [0]	CMOS 3.3V	PD/PU In CPLD		I/O
187	LPC_AD2 / GPIO2	Multiplexed Command, Address and Data/ General purpose input/output [2]	CMOS 3.3V	PD/PU In CPLD		I/O
189	LPC_CLK / GPIO4	LPC clock/ General purpose input/output [2]	CMOS 3.3V	PD/PU In CPLD		I/O
191	SERIRQ / GPIO6	Serialized Interrupt/ General purpose input/output [2]	CMOS 3.3V	PD/PU In CPLD		I/O
193	VCC_RTC	VCC_RTC = 2.4 - 3.3 V	Power			
195	FAN_TACHOIN / GP_TIMER_IN	Fan tachometer input. or can be used as General Purpose Timer Input.	CMOS 3.3V	PU 47 kΩ 3.3V S0		I
197	GND	Power Ground	Power			
199	SPI_MOSI	Master serial output/Slave serial input signal. SPI serial output data from Qseven® module to the SPI device.	CMOS 3.3V			O
201	SPI_MISO	Master serial input/Slave serial output signal. SPI serial input data from the SPI device to Qseven® module.	CMOS 3.3V			I
203	SPI_SCK	SDIO Command/Response - card initialization and command transfers. During initialization mode signal is open drain. During command transfer signal is in push-pull mode.	CMOS 3.3V			O
205	VCC_SB	Standby Power Supply +5VDC ▶+/-5%.	Power			
207	MFG_NC0	Reserved				
209	MFG_NC1	Reserved				
211	NC	Not Connected	NC			
213	NC	Not Connected	NC			
215	NC	Not Connected	NC			
217	NC	Not Connected	NC			
219	VCC	Power Supply +5VDC ▶+/-5%	Power			
221	VCC	Power Supply +5VDC ▶+/-5%	Power			
223	VCC	Power Supply +5VDC ▶+/-5%	Power			
225	VCC	Power Supply +5VDC ▶+/-5%	Power			
227	VCC	Power Supply +5VDC ▶+/-5%	Power			
229	VCC	Power Supply +5VDC ▶+/-5%	Power			

Table 16: QSEVEN® Module Connector Pin Assignment of Top Side Row

Pin	Signal Row (top side)	Description	I/O Type	Termin ation	IOL/ IIL	I/O
2	GND	Power Ground	Power			
4	GBE_MDI2-	Media Dependent Interface (MDI) differential pair 2	GB_LAN			I/O
6	GBE_MDI2+	Media Dependent Interface (MDI) differential pair 2	GB_LAN			I/O
8	GBE_LINK1000#	Ethernet controller 0 1000Mbit/sec link indicator, active low.	CMOS 3.3V PP		Max. 10 mA	O
10	GBE_MDI0-	Media Dependent Interface (MDI) differential pair 0 [1]	GB_LAN			I/O
12	GBE_MDI0+	Media Dependent Interface (MDI) differential pair 0 [1]	GB_LAN			I/O
14	GBE_ACT#	Ethernet controller 0 activity indicator, active low.	CMOS 3.3V PP		Max. 10 mA	O
16	SUS_S5#	S5 State: This signal indicates S4 or S5 (Soft Off) state.	CMOS 3.3V Suspend	PD10 kΩ	≥1mA	O
18	SUS_S3#	S3 State: this signal shuts off power to all runtime system components that are not maintained during S3 (Suspend to Ram), S4 or S5 states. The signal SUS_S3# is necessary in order to support the optional S3 cold power state.	CMOS 3.3V Suspend	PD10 kΩ	≥1 mA	O
20	PWRBTN#	Power button: this signal is a low active input and triggered on the falling edge	CMOS 3.3V Standby	PD/PU in CPLD	≥10 mA	I
22	LID_BTN# / GPII0	LID button: active low signal detects LID switch and brings the module into sleep or wake up state. Open/Close state may be software configurable. Optionally interrupt-capable General Purpose Input 0	CMOS 3.3V Suspend / CMOS 3.3V	PU 10 kΩ 3.3V S5	≥10 mA	I
24	GND	Power Ground	Power			
KEY						
26	PWGIN	Power good: active high input indicated to Qseven® module that all power rails on carrier board are ready for use.	CMOS 5V	PD 100 kΩ	≥4 mA	I
28	RSTBTN#	Reset button is driven active low by external circuitry to reset the Qseven® module	CMOS 3.3V	PD/PU in CPLD	≥10 mA	I
30	SATA1_TX+	SATA channel 1, Transmit Input differential pair	SATA			O
32	SATA1_TX-	SATA channel 1, Transmit Input differential pair	SATA			O
34	GND	Power Ground	Power			
36	SATA1_RX+	SATA channel 1, Receive Input differential pair	SATA			I
38	SATA1_RX-	SATA channel 1, Receive Input differential pair	SATA			I
40	GND	Power Ground	Power			
42	SDIO_CLK#	SDIO Clock. With each cycle of this signal a one-bit transfer on the command and each data line occurs.	CMOS 3.3V			O
44	Reserved	Reserved				
46	SDIO_WP	SDIO Write Protect denotes the state of the write-protect tab on SD cards.	CMOS 3.3V	PU 10 kΩ 3.3V S5		I/O
48	SDIO_DAT1	SDIO Data lines operate in push-pull mode.	CMOS 3.3V PP			I/O
50	SDIO_DAT3	SDIO Data lines operate in push-pull mode.	CMOS 3.3V PP			I/O
52	Reserved	Reserved				
54	Reserved	Reserved				
56	USB_OTG_PEN	USB Power enable pin for USB Port 1 Enables Power for the USB-OTG port on carrier board.	CMOS 3.0V	PD/PU in CPLD		O

Pin	Signal Row (top side)	Description	I/O Type	Termin ation	IOL/ IIL	I/O
58	GND	Power Ground	Power			
60	SMB_CLK / GP1_I2C_CLK	Clock line of System Management Bus Multiplexed with General Purpose I2C bus #1 clock line	CMOS 3.3V OD Suspend	PU 10 kΩ 3.3V S5		I/O
62	SMB_DAT / GP1_I2C_DAT	Data line of System Management Bus Multiplexed with General Purpose I2C bus #1 data line	CMOS 3.3V OD Suspend	PU 10 kΩ 3.3V S5		I/O
64	SMB_ALERT#	System Management Bus Alert input may be driven low by SMB devices to signal an event on the SM Bus.	CMOS 3.3V OD Suspend	PU 10 kΩ 3.3V S5		I/O
66	GP0_I2C_CLK	General Purpose I²C bus #0 clock line	CMOS 3.3V OD	PU 10 kΩ 3.3V S0		I/O
68	GP0_I2C_DAT	General Purpose I²C bus #0 data line	CMOS 3.3V OD	PU 10 kΩ 3.3V S0		I/O
70	WDTRIG#	Watchdog trigger signal restarts the Qseven ® module's watchdog timer on the falling edge of a low active pulse.	CMOS 3.3V	PU 10 kΩ 3.3V S5	≥10mA	I
72	WDOUT	Watchdog event indicator. active high output signs a missing watchdog trigger is deasserted by software, system reset or system power down.	CMOS 3.3V	PU 10 kΩ	Max. 5 mA	O
74	GND	Power Ground	Power			
76	USB_P6- / USB_SSRX0-	Universal Serial Bus Port 6 differential pair / USB Superspeed receive signal differential pair 0	USB			I/O I
78	USB_P6+ / USB_SSRX0+	Universal Serial Bus Port 6 differential pair / USB Superspeed receive signal differential pair 0	USB			I/O I
80	USB_4_5_OC#	Monitors USB power over current of the USB Ports 4 and 5	CMOS 3.3V Suspend	PU 10 kΩ 3.3V S5	≥5 mA	I
82	USB_P4- / USB_SSRX2-	Universal Serial Bus Port 4 differential pair / USB Superspeed receive signal differential pair 2	USB			I/O I
86	USB_0_1_OC#	Monitors USB power over current of the USB Ports 0 and 1	CMOS 3.3V Suspend	PU 10 kΩ 3.3V S5	≥5 mA	I
88	USB_P2-	Universal Serial Bus Port 2 differential pair	USB			I/O
90	USB_P2+	Universal Serial Bus Port 2 differential pair	USB			I/O
92	USB_ID	USB ID pin configures mode of the USB Port 1. The pin's resistance to ground determines whether USB Port 1's USB Client support is Enabled or Disabled	Analogue	PU 100kΩ 3.3V S5		O
94	USB_P0-	Universal Serial Bus Port 0 differential pair	USB			I/O
96	USB_P0+	Universal Serial Bus Port 0 differential pair	USB			I/O
98	GND	Power Ground	Power			
100	eDP1_TX0+ / LVDS_B0+	embedded DP secondary channel differential pair 0 LVDS secondary channel differential pair 0	eDP/DP / LVDS			O
102	eDP1_TX0- / LVDS_B0-	embedded DP secondary channel differential pair 0 LVDS secondary channel differential pair 0.	eDP/DP / LVDS			O
104	eDP1_TX1+ / LVDS_B1+	embedded DP secondary channel differential pair 1 LVDS secondary channel differential pair 1	eDP/DP / LVDS			O
106	eDP1_TX1- / LVDS_B1-	embedded DP secondary channel differential pair 1 LVDS secondary channel differential pair 1	eDP/DP / LVDS			O
108	eDP1_TX2+ / LVDS_B2+	embedded DP secondary channel differential pair 2 LVDS secondary channel differential pair 2	eDP/DP / LVDS			O
110	eDP1_TX2- / LVDS_B2-	embedded DP secondary channel differential pair 2 LVDS secondary channel differential pair 2	eDP/DP / LVDS			O

Pin	Signal Row (top side)	Description	I/O Type	Termination	IOL/ IIL	I/O
112	LVDS_BLEN	Controls panel backlight enable	CMOS 3.3V		Max. 1 mA	O
114	eDP1_TX3+ / LVDS_B3+	embedded DP secondary channel differential pair 3 LVDS secondary channel differential pair 3	eDP/DP / LVDS			O
116	eDP1_TX3- / LVDS_B3-	embedded DP secondary channel differential pair 3 LVDS secondary channel differential pair 3	eDP/DP / LVDS			O
118	GND	Power Ground	Power			
120	eDP1_AUX+ / LVDS_B_CLK+	embedded DisplayPort secondary auxiliary channel. / LVDS secondary channel differential pair clock line	eDP/DP / LVDS			I/O O
122	eDP1_AUX- / LVDS_B_CLK-	embedded DisplayPort secondary auxiliary channel. / LVDS secondary channel differential pair clock line	eDP/DP / LVDS			I/O O
124	GP_1-Wire_Bus / HDMI_CEC	General Purpose 1-Wire bus interface. / or can be used for consumer electronics control bus of HDMI	CMOS 3.3V	PD/PU in CPLD		I/O
126	LVDS_BLC_DAT/ eDP0_HPD#	Control data signal for external SSC clock chip. Or can be used eDP primary Hotplug detection.	CMOS 3.3V OD / CMOS 3.3V OD	PU 10 kΩ 3.3V S5		I/O I
128	LVDS_BLC_CLK / eDP1_HPD#	Control clock signal for external SSC clock chip. Or can be used as eDP secondary Hotplug detection.	CMOS 3.3V OD / CMOS 3.3V OD	PU 10 kΩ 3.3V S5		I/O I
130	CAN0_RX	RX input for CAN Bus channel 0, to connect a CAN controller device to module's CAN bus it is necessary to add transceiver hardware to carrier board.	CMOS 3.3V			I
132	USB_SSTX1-	USB Superspeed transmit signal differential pair	USB			O
134	USB_SSTX1+	USB Superspeed transmit signal differential pair	USB			O
136	GND	Power Ground	Power			
138	DP_AUX+	Auxiliary channel for link management and device control. Differential pair lines.	eDP/DP			I/O
140	DP_AUX-	Auxiliary channel for link management and device control. Differential pair lines.	eDP/DP			I/O
142	GND	Power Ground	Power			
144	USB_SSRX1-	USB Superspeed receive signal differential pair	USB			I
146	USB_SSRX1+	USB Superspeed receive signal differential pair	USB			I
148	GND	Power Ground	Power			
150	HDMI_CTRL_DAT	DDC based control signal (data) for HDMI device. Note: Level shifters must be implemented on carrier board for this signal to be compliant with HDMI Spec.	CMOS 3.3V OD	PU 2.2 kΩ 3.3V S0		I/O
152	HDMI_CTRL_CLK	DDC based control signal (clock) for HDMI device. Note: Level shifters must be implemented on carrier board for signal to be compliant with HDMI Spec.	CMOS 3.3V OD	PU 2.2 kΩ 3.3V S0		I/O
154	DP_HPD#	Hot plug detection signal that serves as an interrupt request.	CMOS 3.3V	PU 100kΩ 3.3V S0		I
156	PCIE_WAKE#	PCI Express Wake Event: Sideband wake signal asserted by components requesting wakeup.	CMOS 3.3V Suspend	PU 10 kΩ 3.3V S5	≥5 mA	I
158	PCIE_RST#	Reset Signal for external devices.	CMOS 3.3V	PD/PU in CPLD	Max. 1 mA	O
160	GND	Power Ground	Power			
162	PCIE3_RX+	PCIe channel 3, Receive Input differential pair	PCIe			I
164	PCIE3_RX-	PCIe channel 3, Receive Input differential pair	PCIe			I

Pin	Signal Row (top side)	Description	I/O Type	Termin ation	IOL/ IIL	I/O
166	GND	Power Ground	Power			
168	PCIE2_RX+	PCIe channel 2, Receive Input differential pair	PCIe			I
170	PCIE2_RX-	PCIe channel 2, Receive Input differential pair	PCIe			I
172	UART0_RTS#	Handshake signal, request to send data	CMOS 3.3V	PD/PU in CPLD	Max. 1 mA	O
174	PCIE1_RX+	PCIe channel 0, Receive Input differential pair	PCIe			I
176	PCIE1_RX-	PCIe channel 0, Receive Input differential pair	PCIe			I
178	UART0_CTS#	Handshake signal, request to send data	CMOS 3.3V	PD/PU in CPLD	≥5 mA	I
180	PCIE0_RX+	PCIe channel 0, Receive Input differential pair	PCIe			I
182	PCIE0_RX-	PCIe channel 0, Receive Input differential pair	PCIe			I
184	GND	Power Ground	Power			
186	LPC_AD1 / GPIO1	Multiplexed Command, Address and Data/ General purpose input/output [1]	CMOS 3.3V	PD/PU In CPLD		I/O
188	LPC_AD3 / GPIO3	Multiplexed Command, Address and Data/ General purpose input/output [3]	CMOS 3.3V	PD/PU In CPLD		I/O
190	LPC_FRAME# / GPIO5	Indicates start of new cycle or termination of broken cycle./ General purpose input/output [5]	CMOS 3.3V	PD/PU In CPLD		I/O
192	LPC_LDRQ# / GPIO7	LPC DMA request / General purpose input/output [7]	CMOS 3.3V	PD/PU In CPLD		I/O
194	SPKR / GP_PWM_OUT2	Primary functionality is output for speaker in systems OR optionally: General Purpose PWM Output.	CMOS 3.3V			O
196	FAN_PWMOUT / GP_PWM_OUT1	Fan speed control. using Pulse Width Modulation (PWM) to control the fan's RPM based on the CPU's die temperature OR optionally as General Purpose PWM Output.	CMOS 3.3V OC	PU 10 kΩ 3.3V S0		O
198	GND	Power Ground	Power			
200	SPI_CS0#	SPI chip select 0 output.	CMOS 3.3V	PU 10 kΩ 3.3V S5		O
202	SPI_CS1#	SPI Chip Select 1 signal is used as the second chip select when two devices are used. Do not use when only one SPI device is used.	CMOS 3.3V	PU 10 kΩ 3.3V S5		O
204	MFG_NC4	Reserved				
206	VCC_SB	Standby Power Supply +5VDC ±5%.	Power			
208	MFG_NC2	Reserved				
210	MFG_NC3	Reserved				
212	NC	Not Connected	NC			
214	NC	Not Connected	NC			
216	NC	Not Connected	NC			
218	NC	Not Connected	NC			
220	VCC	Power Supply +5VDC ▶+/-5%.	Power			
222	VCC	Power Supply +5VDC ▶+/-5%.	Power			
224	VCC	Power Supply +5VDC ▶+/-5%.	Power			
226	VCC	Power Supply +5VDC ▶+/-5%.	Power			
228	VCC	Power Supply +5VDC ▶+/-5%.	Power			
230	VCC	Power Supply +5VDC ▶+/-5%.	Power			

9/ Power on

The Q7ALx2 module receives power from a carrier board via the Qseven® connector. The Q7ALx2 must be connected to a carrier board to power on and power off.

⚠CAUTION

A carrier board powers the module by means of the Qseven® connector. Before connecting the module to the corresponding connector on the carrier board, switch off and disconnect the main power supply. Failure to disconnect the main power supply could result in personal injury and damage to the module and/or carrier board.

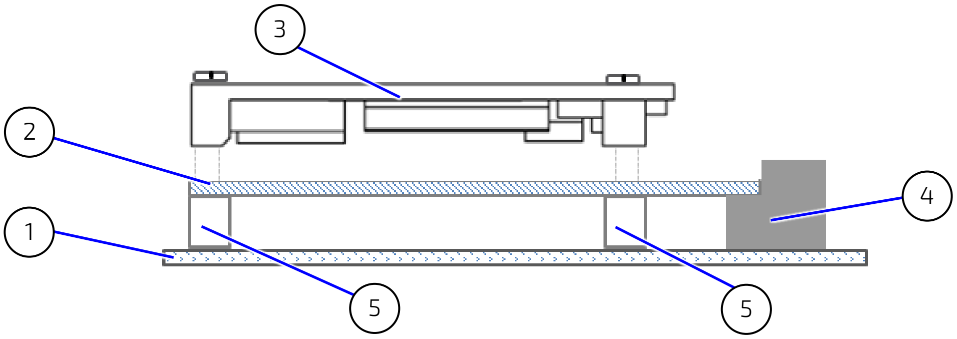
⚠CAUTION

Handling and operation of the product is permitted only for trained personnel within a work place that is access controlled.

9.1. Connecting to the Carrier Board

The Q7ALx2 module connects to a carrier board via the carrier boards Qseven® connector the height of the standoffs between the carrier board and the module depends on the height of the Qseven® connector. The heatspreader plate features boss extrusions as standoffs for precise installation on the module's four mounting points.

Figure 12: Qseven® Module with Carrier Board Assembly with Heatspreader Plate



1	Carrier board	4	Qseven® connector
2	Q7ALx2 module	5	Standoffs (not supplied with module)
3	Heatspreader plate		

To connect the Q7ALx2 module to the carrier board perform the following:

1. Switch off the power to the carrier board and disconnect the carrier board from the main power supply. Failure to disconnect the main power supply could result in personal injury and damage to the module and/or carrier board.
2. Insert the module's Qseven® connector (Figure 3, pos. 3 and Figure 4, pos. 1), with the top side facing upwards, into a carrier board's corresponding Qseven® connector (Figure 12, pos.4).
3. Secure the module to the carrier board using the four mounting points (Figure 3, pos. 6 and Figure 4, pos. 2) with standoffs. Note: The height of the required standoffs depends on the height of the carrier board's Qseven® connector.
4. Position and secures the module's heatspreader plate carefully, with the thermal pads on the underside of the heatspreader on top of the module's major heat-generating components (Figure 12, pos. 3).
5. Connect the carrier board to the main power supply and switch on the carrier board to power on the module or switch off the carrier board to power off the module.

10/ uEFI BIOS

10.1. Starting the uEFI BIOS

The Q7ALx2 module uses a Kontron-customized, pre-installed and configured version of Aptio ® V uEFI BIOS based on the Unified Extensible Firmware Interface (uEFI) specification and the Intel® Platform Innovation Framework for EFI. The uEFI BIOS provides a variety of new and enhanced functions specifically tailored to the hardware features of the Q7ALx2 module.

The BIOS features in this user guide are open to change and may not be the latest version. The latest version may have differences to the options and features described in this chapter.

Register for the EMD Customer Section to get access to BIOS downloads and PCN service.

The uEFI BIOS setup program provides quick and easy access to the individual function settings for control or modification of the uEFI BIOS configuration. The setup program allows for access to various menus that provide functions or access to sub-menus with further specific functions of their own.

To start the uEFI BIOS setup program, follow the steps below:

1. Power on the module, see Chapter 9/Power on.
2. Wait until the first characters appear on the screen (POST messages or splash screen).
3. Press the <DEL> key.
4. If the uEFI BIOS is password-protected, a request for password will appear. Enter either the User Password or the Supervisor Password (see Chapter 10.2.4 Security Setup Menu), press <RETURN>, and proceed with step 5.
5. A setup menu appears.

The uEFI BIOS setup program uses a hot key navigation system. The hot key legend bar is located at the bottom of the setup screens. The following table provides a list of navigation hot keys available in the legend bar.

Table 17: Navigation Hot Keys in the Legend Bar

Sub-screen	Description
<F1>	<F1> key invokes the General Help window
<->	<Minus> key selects the next lower value within a field
<+>	<Plus> key selects the next higher value within a field
<F2>	<F2> key loads previous values
<F3>	<F3> key loads optimized defaults
<F4>	<F4> key Saves and Exits
<→> or <←>	<Left/Right> arrows selects major Setup menus on menu bar, for example, Main or Advanced
<↑> or <↓>	<Up/Down> arrows select fields in the current menu, for example, Setup function or sub-screen
<ESC>	<ESC> key exits a major Setup menu and enters the Exit Setup menu Pressing the <ESC> key in a sub-menu displays the next higher menu level
<RETURN>	<RETURN> key executes a command or selects a submenu

10.2. Setup Menus

The Setup utility features menus listed in the selection bar at the top of the screen are:

- Main
- Advanced
- Chipset
- Security
- Boot
- Save & Exit

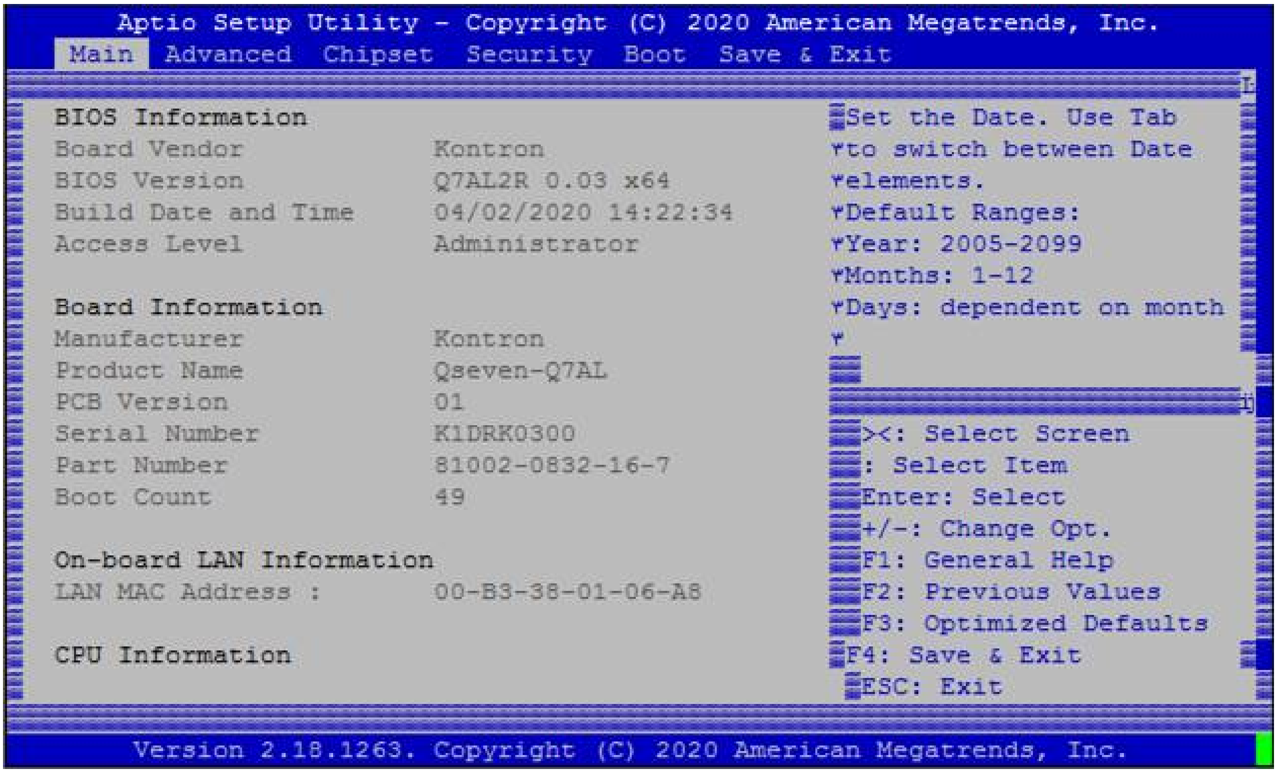
The currently active menu and the currently active uEFI BIOS setup item are highlighted in white. Use the left and right arrow keys to select the setup menu.

Each setup menu provides two main frames. The left frame displays all available functions. Configurable functions are displayed in blue. Functions displayed in grey provide information about the status or the operational configuration. The right frame displays a Help window providing an explanation of the respective function.

10.2.1. Main Setup Menu

On entering the uEFI BIOS, the setup program displays the Main setup menu. This screen lists the Main setup menu sub-screens and provides basic system information as well as functions for setting the system language, time and date.

Figure 13: Main Setup Menu Initial Screen Example



```
       Aptio Setup Utility - Copyright (C) 2020 American Megatrends, Inc.
   Main  Advanced  Chipset  Security  Boot  Save & Exit

   BIOS Information                                 Set the Date. Use Tab
   Board Vendor            Kontron                  to switch between Date
   BIOS Version            Q7AL2R 0.03 x64          elements.
   Build Date and Time     04/02/2020 14:22:34      Default Ranges:
   Access Level            Administrator            Year: 2005-2099
                                                    Months: 1-12
   Board Information                                Days: dependent on month
   Manufacturer            Kontron
   Product Name            Qseven-Q7AL
   PCB Version             01
   Serial Number           K1DRK0300                ><: Select Screen
   Part Number             81002-0832-16-7          : Select Item
   Boot Count              49                       Enter: Select
                                                    +/-: Change Opt.
   On-board LAN Information                         F1: General Help
   LAN MAC Address :       00-B3-38-01-06-A8        F2: Previous Values
                                                    F3: Optimized Defaults
   CPU Information                                  F4: Save & Exit
                                                    ESC: Exit

       Version 2.18.1263. Copyright (C) 2020 American Megatrends, Inc.
```

The following table shows the Main setup menu sub-screens and functions and describes the content.

The BIOS features in this user guide are open to change and may not be the latest version. The latest version may have differences to the options and features described in Table 18.

Table 18: Main Setup Menu Sub-screens and Functions Example

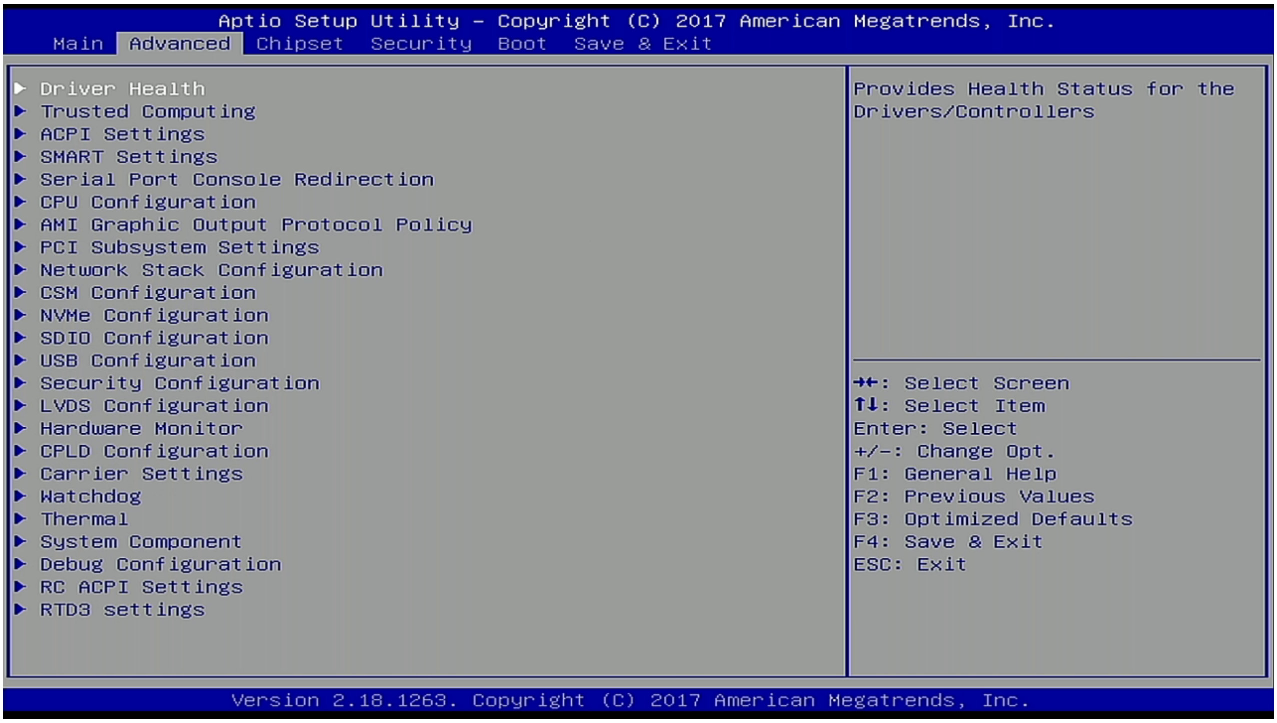
Sub-Screen	Description
BIOS Information>	Read only field BIOS vendor, Core version, Compliancy, Project version, Build date and time, and Access level
On-board LAN Information>	Read only field LAN MAC Address **Additional information for MAC Address** The MAC address entry is the value used by the Ethernet controller and may contain the entry 'Inactive' - Ethernet chip is inactive. To activate the Ethernet chip set the following: Advanced > Network Stack Configuration > Network Stack > Enable 88:88:88:88:87:88 is a special pattern that will be filled in by the Ethernet firmware if there is no valid entry in the firmware block of the BIOS SPI (i.e. the MAC address has been overwritten during the last attempt to flash the system).
CPU Information>	Read only field Processor Type, CPU signature, Microcode patch, CPU Speed, processor Core, intel VT-x technology
Memory Information>	Read only field Total memory and Memory speed
Platform Firmware Information>	Read only field *Module Information* BXT SOC, MRC Version, PUNIT FW, PMC FW, TXE FW, GOP, and CPLD rev
System Date>	Displays the system date [Week day mm/dd/yyyy]
System Time>	Displays the system time [hh:mm:ss]

10.2.2. Advanced Setup Menu

The Advanced setup menu displays sub-screens and second level sub-screens with functions, for advanced configurations.

NOTICE Setting items, on this screen, to incorrect values may cause system malfunctions.

Figure 14: Advanced Setup Menu Initial Screen Example



```
          Aptio Setup Utility – Copyright (C) 2017 American Megatrends, Inc.
    Main  Advanced  Chipset  Security  Boot  Save & Exit

 ▶ Driver Health                                     Provides Health Status for the
 ▶ Trusted Computing                                 Drivers/Controllers
 ▶ ACPI Settings
 ▶ SMART Settings
 ▶ Serial Port Console Redirection
 ▶ CPU Configuration
 ▶ AMI Graphic Output Protocol Policy
 ▶ PCI Subsystem Settings
 ▶ Network Stack Configuration
 ▶ CSM Configuration
 ▶ NVMe Configuration
 ▶ SDIO Configuration
 ▶ USB Configuration
 ▶ Security Configuration                            →←: Select Screen
 ▶ LVDS Configuration                                ↑↓: Select Item
 ▶ Hardware Monitor                                  Enter: Select
 ▶ CPLD Configuration                                +/-: Change Opt.
 ▶ Carrier Settings                                  F1: General Help
 ▶ Watchdog                                          F2: Previous Values
 ▶ Thermal                                           F3: Optimized Defaults
 ▶ System Component                                  F4: Save & Exit
 ▶ Debug Configuration                               ESC: Exit
 ▶ RC ACPI Settings
 ▶ RTD3 settings

             Version 2.18.1263. Copyright (C) 2017 American Megatrends, Inc.
```

The following table shows the Advanced sub-screens and functions and describes the content. Default settings are in **bold** and for some functions, additional information is included.

The BIOS features in this user guide are open to change and may not be the latest version. The latest version may have differences to the options and features described in Table 19.

Table 19: Advanced Setup menu Sub-screens and Functions Example

Sub-Screen	Function	Second level Sub-Screen / Description
Driver Health>	Read only Information Provides Health Status for the Drivers/Controllers	
Trusted Computing>	Read only Information TPM20 device Found, Vendor and Firmware version	
	Security Device Support>	Enables or disables BIOS support for security device Operating System will not show security device, and TCG EFI protocol and INT1A interface are not available. [**Enabled**, Disabled]
	Active PCR Banks>	Read only field Displays active PCR Banks

Sub-Screen	Function	Second level Sub-Screen / Description
Trusted Computing> (continued)	Available PCR Banks>	Read only field Displays available PCR Banks
	SHA-1 PCR Bank>	SHA-1 PCR Bank [**Enabled**, Disabled]
	SHA256 PCR Bank>	SHA256 PCR Bank [**Enabled**, Disabled]
	Pending Operation>	Schedules an operation for security device Note: Computer reboots on restart to change the state of the security device. [**None**, TPM Clear]
	Platform Hierarchy>	Platform Hierarchy [**Enabled**, Disabled]
	Storage Hierarchy>	Storage Hierarchy [**Enabled**, Disabled]
	Endorsement Hierarchy>	Endorsement Hierarchy [**Enabled**, Disabled]
	TPM2.0 UEFI Spec Version>	Selects TCG2 Spec Version support TCG_1_2: is compatible mode for Win8/Win10 and TCG_2: supports TCG2 protocol and event format Win 10 or later. [TCG_1_2, **TCG_2**]
	Physical Presence Spec Version>	Select to inform OS to support either PPI Spec 1.2 or 1.3 Note: Some HCK tests might not support 1.3. [1.2, **1.3**]
	TPM 20 InterfaceType>	Read only field
	Device Select>	Selects BIOS support for security devices. Auto: supports both TPM 1.2 and TPM 2.0 TPM 1.2: restricts support to TPM 1.2 devices TPM 2.0: restricts support to TPM 2.0 devices [TPM 1.2, TPM 2.0, **Auto**]
ACPI Settings>	Enable ACPI Auto Configuration>	Enables or disables BIOS ACPI auto configuration. If enabled, the system uses generic ACPI settings that may not fit the system best. [Enabled, **Disabled**]
	Enable Hibernation>	Enables or disables systems ability to hibernate (OS/S4 Sleep State) This option may not be effective with some operating systems. [**Enabled**, Disabled]
	ACPI Sleep State>	Selects highest ACPI sleep state the system enters when the SUSPEND button is pressed [Suspend Disabled, **S3 Suspend to Ram**]
	Lock Legacy Resources>	Lock of legacy resources [Enabled, **Disabled**]
SMART Settings>	SMART Self Test>	Run SMART Self Test on all HDDs during POST [Enabled, **Disabled**]
Serial Port Console Redirection>	COM0 Console Redirection>	Console redirection via QSEVEN module's COM1 [Enabled, **Disabled**]
	COM1 Console Redirection>	Console redirection via QSEVEN module's COM2 [Enabled, **Disabled**]

Sub-Screen	Function	Second level Sub-Screen / Description
Serial Port Console Redirection> (continued)	COM2 Console Redirection>	Console redirection via QSEVEN module's COM3 [Enabled, **Disabled**]
	COM3 Console Redirection>	Console redirection via QSEVEN module's COM4 [Enabled, **Disabled**]
	Additional Information COM # Console If redirection is enabled then the port settings such as Terminal type, Bits per second, Data bits, Parity etc. can be adjusted here. On-module COM ports do not support flow control. If the Port is disabled, the COM# port is displayed as a read only field.	
	Legacy Console Redirection settings>	Legacy Serial Redirection Port> Selects a COM port to display redirection of legacy OS and legacy OPROM messages [**COM0**, COM1, COM2, COM3]
	Serial Port for Out-of-Band Management / Windows EMS Console Redir.>	Console redirection [Enabled, **Disabled**]
CPU Configuration>	Turbo Mode>	Enables or disables processor turbo mode Note: EMTTM must also be enabled. Auto means enabled unless the max. turbo ratio is bigger than 16-SKL A0 W/A. [**Enabled**, Disabled]
	Intel (VME) Virtual Technology>	Enables VMM to utilize additional hardware capabilities provided by Vanderpool Technology [**Enabled**, Disabled]
	VT-d>	CPU VT-d [Enabled, **Disabled**]
	Monitor Mwait>	Monitor Mwait [Enabled, **Disabled**, Auto]
AMI Graphic Output Protocol Policy>	Read only field AMI Graphic driver version	
	Output Select>	
PCI Subsystem Settings>	Read only field AMI PCI driver version	
	Above 4G Decoding>	64 bit capable devices to be decoded in above 4G address space [Enabled, **Disabled**]
	Hot-Plug Support>	Hot-Plug support for the entire system [**Enabled**, Disabled]
Network Stack Configuration>	Network Stack>	UEFI Network Stack [Enabled, **Disabled**]
Compatibility Support Module (CSM) Configuration	CSM Support>	CSM Support [Enabled, **Disabled**]
NVMe Configuration>	Read only field NVMe controller and driver version	
SDIO Configuration>	SDIO Access Mode>	Auto Option: Access SD device in DMA mode if controller supports it, otherwise in PIO mode. DMA option: Access SD device in DMA mode. PIO Option: Access SD device in PIO mode.

Sub-Screen	Function	Second level Sub-Screen / Description
SDIO Configuration> (continued)	SDIO Access Mode> (continued)	[**Auto**, ADMA, SDMA, PIO]
	Mass storage devices>	Mass storage device emulation type. [**Auto**, Floppy, Forced FDD, Hard Disk]
USB Configuration>	Read only fields USB Configuration, UBS module Version, USB controllers, and USB devices	
	Legacy USB Support>	Enable- supports legacy USB Auto– disables legacy support, if no USB devices are connected Disable-keeps USB devices available for EFI applications only [**Enabled**, Disabled, Auto]
	XHCI Hand-off>	XHCI ownership change claimed by XHCI driver. Note: This is a work around for OS(s) without XHCI hand-off support. [**Enabled,** Disabled]
	USB Mass Storage Driver Support>	Enables or disables USB mass storage driver support [**Enabled,** Disabled]
	USB Transfer Time-out>	Displays timeout value for control, bulk and interrupt transfers [1 sec, 5 sec, 10 sec, **20 sec**]
	Device Reset Time-out>	Displays USB mass storage device start unit command time-out [10 sec, **20 sec**, 30 sec, 40 sec]
	Device Power-up Delay>	Displays maximum time taken for the device to report itself to the host properly. Auto uses the default :root port 100 ms /hub port delay is taken from hub port descriptor. [**Auto**, Manual]
	Mass Storage Devices>	Mass storage device emulation type [**Auto**, Floppy, Forced FDD, Hard Disk, CD-ROM]
Security Configuration>	TXE HMRFPO>	TXE HMRFPO [Enabled, **Disabled]**
	TXE EOP Message>	Send EOP Message before enter OS [**Enabled,** Disabled]
LVDS Configuration>	LVDS Flat Panel Display Support>	Enables or disables the LVDS Flat Panel Display Support [Enabled, **Disabled]**
Hardware Monitor>	CPU Temperature>	Read only field CPU temperature (°C)
	PCB Temperature>	Read only field PCB temperature (°C)
	Module Temperature>	Read only field Module temperature (°C)
	Module Voltage>	Read only field Module voltage (V)
	RTC Voltage>	Read only field RTC Voltage (V)
	DDR Voltage>	Read only field DDR Voltage (V)
	Input Voltage>	Read only field Input Voltage (V)

Sub-Screen	Function	Second level Sub-Screen / Description
Hardware Monitor> (continued)	System Fan – Fan Pulse>	Displays number of pulses the fan produces during one revolution. (Range: 1-4)
	System Fan - Control Mode>	Sets System Fan Control mode [Manual, SMART FAN IV]
	System Fan – Fan Trip Point>	Displays temperature at which the fan accelerates. (Range: 20°C – 80°C)
	System Fan – Trip Point Speed>	Displays Fan speed at trip point in %. Minimum value is 30 %. Fan always runs at 100 % at (TJmax.-10°C).
CPLD Configuration>	Serial Port 0>	Enables or disables the LVDS Flat Panel Display Support [**Enabled**, Disabled]
	Base Address>	Configure Serial Port Base Address [3F8, 2F8, **3E8**, 2E8]
	IRQ>	Configure Serial Port IRQ [7, 9, **10**, 11, 12, 13, 15]
	GPIO IRQ>	Configure IRQ for GPIO pins [Disabled, 9, 10, 11, 12, 13, 15]
	I2C IRQ>	Configure IRQ for I2C Controller [Disabled, 9, 10, 11, 12, 13, 15]
	Audio Codec Mux Select>	Mux select for Audio Codec type on Carrier Board [Mux to I2S Codec, Mux to HDA Codec]
	GPIO-LPC Mux Select>	MUX select for pin as GPIO or LPC Bus to pass through to carrier board [Mux to LPC, Mux to GPIO]
	GPI0 Mux Select>	MUX select for the pin as GPIO or SUS_STAT [Mux to GPIO, Mux to SUS_STAT#]
Carrier Settings>	Carrier I2C0/SMBUS>	Switch to select which controller own the I2C_PM_CK & I2C_PM_DAT pins on Qseven connector [Use I2C0 Controller, Use SMBUS Controller]
	Lid Switch Mode>	Shows or hides Lid switch inside ACPI OS [**Enabled**, Disabled]
	Sleep Button Mode>	Shows or hides Sleep button inside ACPI OS [**Enabled**, Disabled]
Watchdog>	Auto Reload>	Enables automatic reload of watchdog timers on timeout [Enabled, **Disabled**]
	Global Lock>	Enable sets all Watchdog registers (except for WD_KICK) to read only, until the module is reset. [Enabled, **Disabled**]
	Stage 1 Mode>	Selects action for Watchdog stage 1 [**Disable**, Reset, NIM, SCI, Delay, WDT Signal only]
Thermal Configuration Parameters>	Automatic Thermal Reporting>	Configure _CRT, _PSV and _AC0 automatically based on values recommended in BWG's Thermal Reporting [Enabled, **Disabled**]
	Passive Trip Point>	Configure temperature value of the ACPI Passive Trip Point – point which OS will begin throttling the processor. [Disable, 15°C, 23°C, 31°C, 39°C, 47°C, 55°C, 63°C, 71°C, 79°C, 87°C, **95°C**, 103°C, 111°C]
	Passive TC1 Value>	Sets the TC1 value for the ACPI Passive Cooling Formula. (Range: 1 – 6)

Sub-Screen	Function	Second level Sub-Screen / Description
Thermal Configuration Parameters> (continued)	Passive TC2 Value>	Sets TC2 value for the ACPI Passive Cooling Formula.(Range: 1 – 16)
	Passive TSP Value>	Sets TSP value for the ACPI Passive Cooling Formula.(Range: 2 – 32)
System Component>	OS Reset Selet>	Select the reset type in FACP table [Warm Reset, **Cold Reset**]
	Spread Spectrum Clocking Configuration (SSC)	
	DDR SSC>	Enable DDR SSC [**Enable**, Disable]
	DDR SSC Selection Table>	Select the item in SSC selection table for DDR spread spectrum [0% (No SSC), -0.1%, -0.2%, -0.3%, -0.4%, **-0.5%**,]
	DDR Clock Bending Selection Table>	Select Clock Bending [1.3%, 0.6%, **0% (No Clock Bending)**, -0.9%]
	HighSpeed SerialIO SSC>	Enable HighSpeed SerialIO SSC configuration [**Enable**, Disable]
	HighSpeed SerialIO SSC Selection T>	Select the item in SSC selection table for HighSpeed SerialIO spread spectrum [0% (No SSC), -0.1%, -0.2%, -0.3%, -0.4%, **-0.5%**,]
Debug Configuration>	Kernel Debugger Enable>	Enable or disable support for a kernel debugger [Enable, **Disable**]
	APEI BERT>	Enable or disable APEI BERT [**Enable**, Disable]
	ACPI Memory Debug>	Enable or disable ACPI Memory Debug [Enable, **Disable**]
	End Of Post (TXE Debug)>	Disable to stop BIOS from sending End of Post Message [**Enabled**, Disabled]
	Lock Directory (TXE Debug)>	Enable BIOS to lock SETUP variable after end of post [Enabled, **Disabled**]
	Suppress PTT Commands>	Bypass TPM2 commands submitting to PTT FW [Enabled, **Disabled**]
	TDO GPIO Pin>	If select Auto, TDO will be disabled for A0 silicon only. For other steppings, TDO will be enabled. [Enable, Disable, Auto]
	Max Memory 2G>	Set Maximum Memory Size to 2 GB [Enable, **Disable**]
	Persistent RAM size>	Specify the amount of main memory to be reserved for Pram. [4MB, 16MB, 64MB, **Disable**]
	OS DnX focus entry>	Enable OS Dnx [Enable, **Disable**]
	Processor Trace Memory Allocation>	Disable or Select Processor trace memory region size : from 4 KB to 128 MB [**Disabled**, 4KB, 8KB, 16KB, 32KB, 64KB, 128KB, 256KB, 512KB, 1MB, 2MB, 4MB, 8MB, 16MB, 32MB, 64MB, 128MB]
	CSE Data Clear>	Data Clear is for reset/clearing of the CSE data region
RC ACPI Setting>	Native PCIE Enable>	Enable or disable PCI Express Native Control in Windows [**Enable**, Disable]

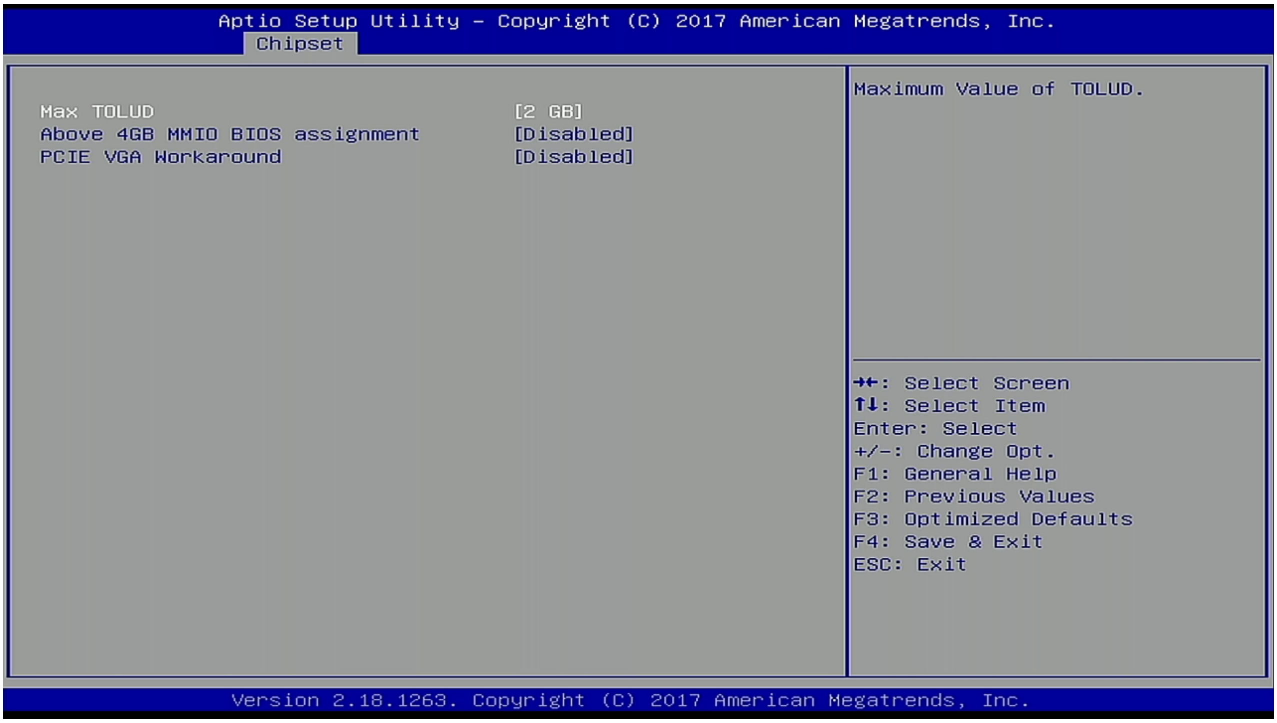
Sub-Screen	Function	Second level Sub-Screen / Description
RC ACPI Setting> (continued)	Native ASPM>	On enable, windows will control the ASPM support for the device. If disabled, the BIOS will [**Enable**, Disable]
RTD3 Settings>	RTD3 Support>	Enable or disable Runtime D3 support [Enabled, **Disabled**]

10.2.3. Chipset Setup Menu

The Chipset setup menu lists four sub-screen options North bridge, South bridge, Uncore Configuration and South Cluster Configuration.

10.2.3.1. Chipset> North Bridge

Figure 15: Chipset > North Bridge Menu Initial Screen Example



```
Aptio Setup Utility – Copyright (C) 2017 American Megatrends, Inc.
Chipset

Max TOLUD                                   [2 GB]
Above 4GB MMIO BIOS assignment              [Disabled]
PCIE VGA Workaround                         [Disabled]

Maximum Value of TOLUD.

→←: Select Screen
↑↓: Select Item
Enter: Select
+/-: Change Opt.
F1: General Help
F2: Previous Values
F3: Optimized Defaults
F4: Save & Exit
ESC: Exit

Version 2.18.1263. Copyright (C) 2017 American Megatrends, Inc.
```

The following table shows the North bridge sub-screens and functions and describes the content. Default settings are in **bold**.

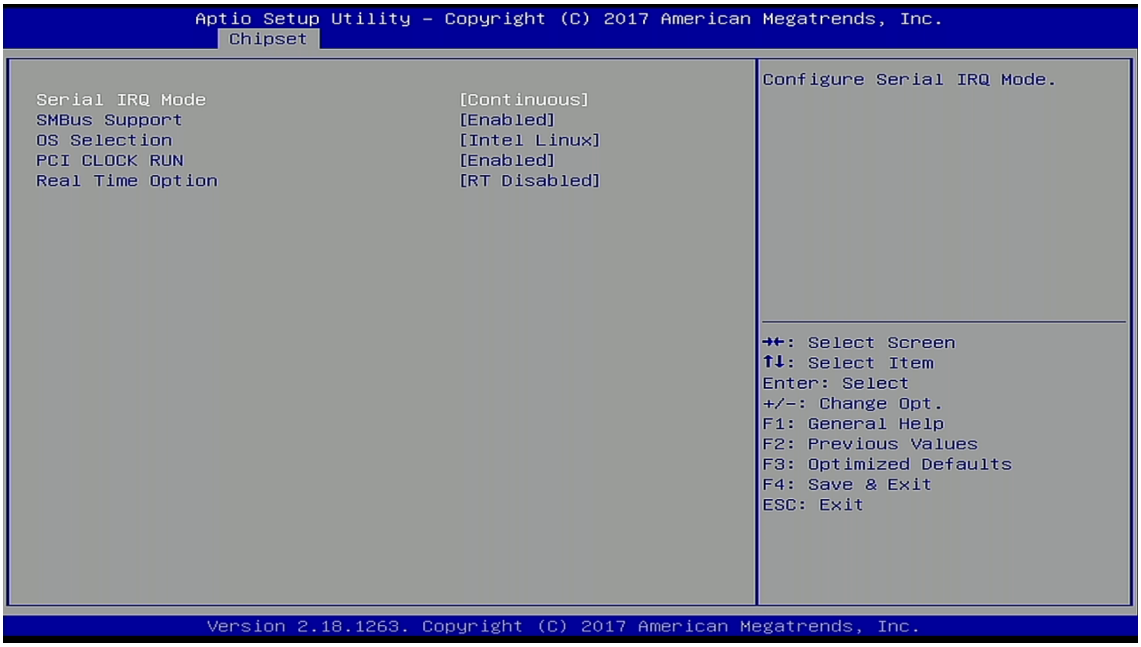
The BIOS features in this user guide are open to change and may not be the latest version. The latest version may have differences to the options and features described in Table 20.

Table 20: Chipset Set > North Bridge Sub-screens and Function

Function	Second level Sub-Screen / Description	
Memory Configuration>	Max TOLUD>	Sets the maximum TOLUD value. Dynamic assignment adjusts TOLUD automatically, based on largest MMIO length of the installed graphic controller. [**2 GB**, 2.25 GB, 2.5 GB, 2,75 GB, 3 GB]
	Above 4GB MMIO BIOS Assignment>	Enables or disables above 4 GB memorymappedIO BIOS assignment. This is disabled automatically when aperture size is set to 2048 MB. [Enabled, **Disabled**]
	PCIE VGA Workaround>	Enable If PCIe card cannot boot in DOS. For test purposes only. [Enabled, **Disabled**]

10.2.3.2. Chipset > South Bridge

Figure 16: Chipset>South Bridge Menu Initial Screen Example



```
          Aptio Setup Utility – Copyright (C) 2017 American Megatrends, Inc.
                 Chipset

 Serial IRQ Mode                       [Continuous]      Configure Serial IRQ Mode.
 SMBus Support                         [Enabled]
 OS Selection                          [Intel Linux]
 PCI CLOCK RUN                         [Enabled]
 Real Time Option                      [RT Disabled]

                                                         →←: Select Screen
                                                         ↑↓: Select Item
                                                         Enter: Select
                                                         +/-: Change Opt.
                                                         F1: General Help
                                                         F2: Previous Values
                                                         F3: Optimized Defaults
                                                         F4: Save & Exit
                                                         ESC: Exit

          Version 2.18.1263. Copyright (C) 2017 American Megatrends, Inc.
```

The following table shows the South Bridge sub-screens and functions, and describes the content. Default settings are in **bold**.

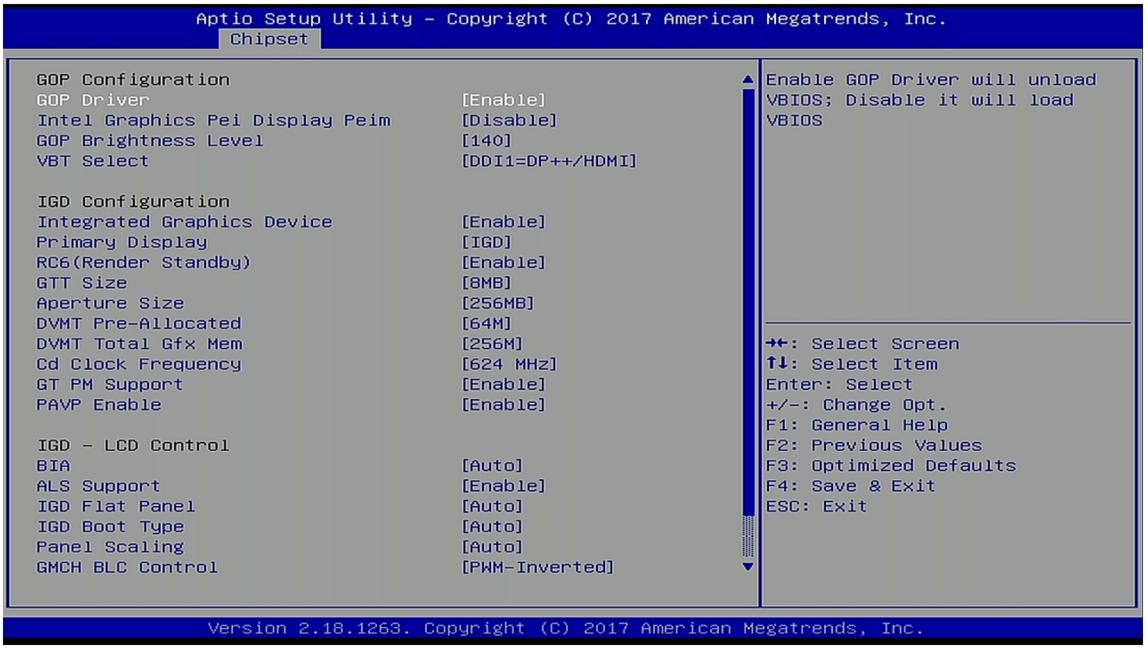
The BIOS features in this user guide are open to change and may not be the latest version. The latest version may have differences to the options and features described in Table 21.

Table 21: Chipset Set> South Bridge Sub-screens and Functions

Function	Second level Sub-Screen / Description
Serial IRQ Mode>	Configure Serial IRQ Mode [Quiet, **Continuous**]
SMBus Support>	Enable or disable SMBus Support [**Enabled**, Disabled]
OS Selection>	Selects target OS. [Windows 10 (Ver>=1607), **Intel Linux**]
PCI Clock Run>	Enables CLKRUN# logic to stop PCI clocks [**Enabled**, Disabled]
Real Time Option>	Select Read-Time Enable and IDI Agent Real-Time Traffic Mask Bits [**RT Disabled**, RT Enabled (Agent IDI1), RT Enabled (Agent Disabled)]

10.2.3.3. Chipset> Uncore Configuration

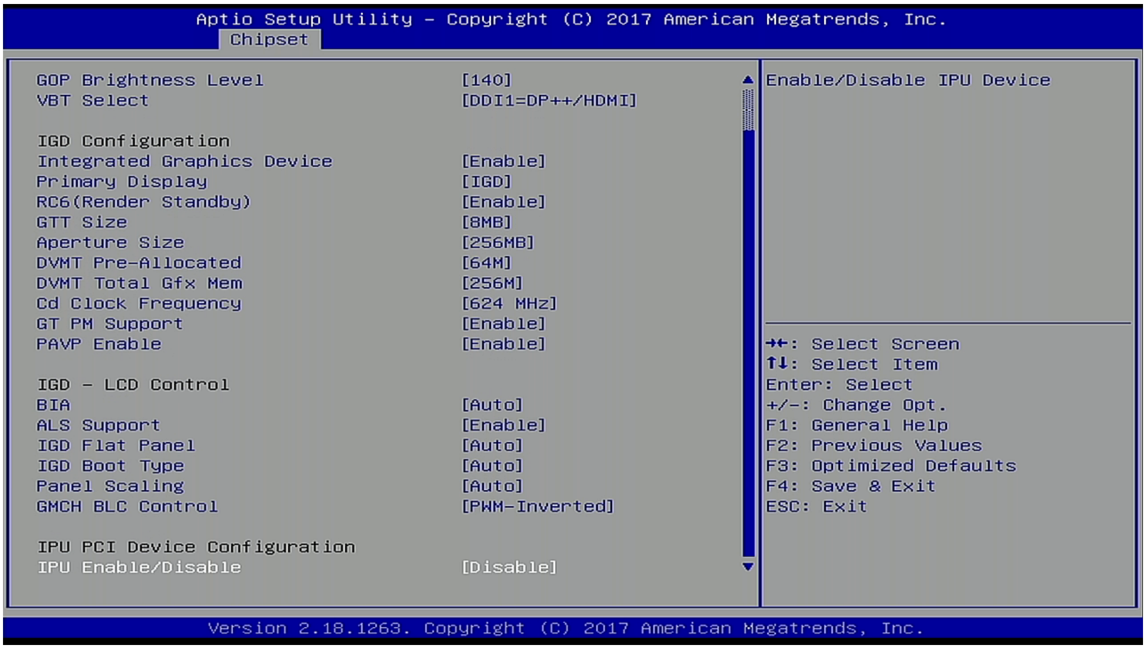
Figure 17: Chipset>Uncore Configuration Menu Initial Screen Examples



```
         Aptio Setup Utility – Copyright (C) 2017 American Megatrends, Inc.
                Chipset
  GOP Configuration                                  Enable GOP Driver will unload
  GOP Driver                    [Enable]             VBIOS; Disable it will load
  Intel Graphics Pei Display Peim [Disable]          VBIOS
  GOP Brightness Level          [140]
  VBT Select                    [DDI1=DP++/HDMI]

  IGD Configuration
  Integrated Graphics Device    [Enable]
  Primary Display               [IGD]
  RC6(Render Standby)           [Enable]
  GTT Size                      [8MB]
  Aperture Size                 [256MB]
  DVMT Pre-Allocated            [64M]
  DVMT Total Gfx Mem            [256M]               →←: Select Screen
  Cd Clock Frequency            [624 MHz]            ↑↓: Select Item
  GT PM Support                 [Enable]             Enter: Select
  PAVP Enable                   [Enable]             +/-: Change Opt.
                                                     F1: General Help
  IGD - LCD Control                                  F2: Previous Values
  BIA                           [Auto]               F3: Optimized Defaults
  ALS Support                   [Enable]             F4: Save & Exit
  IGD Flat Panel                [Auto]               ESC: Exit
  IGD Boot Type                 [Auto]
  Panel Scaling                 [Auto]
  GMCH BLC Control              [PWM-Inverted]

          Version 2.18.1263. Copyright (C) 2017 American Megatrends, Inc.
```



```
         Aptio Setup Utility – Copyright (C) 2017 American Megatrends, Inc.
                Chipset
  GOP Brightness Level          [140]                Enable/Disable IPU Device
  VBT Select                    [DDI1=DP++/HDMI]

  IGD Configuration
  Integrated Graphics Device    [Enable]
  Primary Display               [IGD]
  RC6(Render Standby)           [Enable]
  GTT Size                      [8MB]
  Aperture Size                 [256MB]
  DVMT Pre-Allocated            [64M]
  DVMT Total Gfx Mem            [256M]
  Cd Clock Frequency            [624 MHz]
  GT PM Support                 [Enable]
  PAVP Enable                   [Enable]             →←: Select Screen
                                                     ↑↓: Select Item
  IGD - LCD Control                                  Enter: Select
  BIA                           [Auto]               +/-: Change Opt.
  ALS Support                   [Enable]             F1: General Help
  IGD Flat Panel                [Auto]               F2: Previous Values
  IGD Boot Type                 [Auto]               F3: Optimized Defaults
  Panel Scaling                 [Auto]               F4: Save & Exit
  GMCH BLC Control              [PWM-Inverted]       ESC: Exit

  IPU PCI Device Configuration
  IPU Enable/Disable            [Disable]

          Version 2.18.1263. Copyright (C) 2017 American Megatrends, Inc.
```

The following table shows the Uncore Configuration sub-screens and functions and describes the content. Default settings are in **bold**.

The setup menu screens may not be the latest version. The latest version may have certain differences to the options and features described in Table 22.

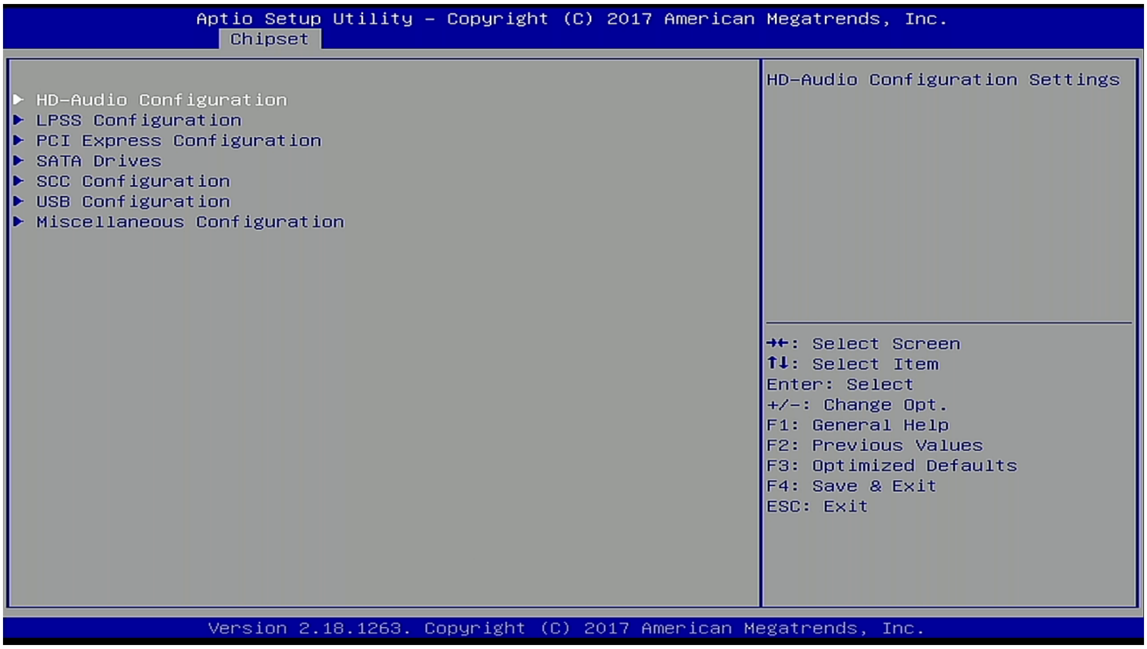
Table 22: Chipset Set> Uncore Configuration Sub-screens and Functions

Function	Second level Sub-Screen / Description
GOP Driver>	Enable GOP Driver will unload VBIOS; Disable it will load VBIOS [**Enabled**, Disabled]
Intel Graphics Pei Display Peim>	Enable or disable Pei (Early) Display [Enabled, **Disabled**]
GOP Brightness Level>	Set GOP Brightness Level; (Range: 0 – 255) [20, 40, 60, 80, 100, 120, **140**, 160, 180, 200, 220, 240, 255]
VBT Select>	Select VBT for GOP Driver [DDI1=DP++/HDMI, DDI1=HDMI]
Integrated Graphics Device (IGD)>	Enable: Enable IGD when selected as the Primary Video Adaptor; Disable: Always disable IGD [**Enabled**, Disabled]
Primary Display>	Select which of IGD/PCI Graphics device should be Primary Display [**IGD**, PCIe, HG]
RC6 (render Standby)>	Check to enable render standby support. IF S0ix is enabled, RC6 should be enabled. This function is read only if S0ix is enabled. [**Enabled**, Disabled]
GTT Size>	Selects the GTT size [2 MB, 4 MB, **8 MB**]
Aperature Size>	Selects the aperture size [128 MB, **256 MB**, 512 MB]
DVMT Pre-Allocated>	Selects DVMT 5.0 pre-allocated (fixed) graphics memory size used by Internal graphics [**64 M**, 96 M, 128 M, 160 M, 192 M, 224 M, 256 M, 288 M, 320 M, 352 M 384 M, 416 M, 448 M, 480M, 512 M]
DVMT Total Gfx Mem>	Selects DVMT 5.0 total graphics memory size used by internal graphics device [128 M, **256 M**, MAX]
Cd Clock Frequency>	Selects the highest Cd clock frequency supported by the platform [144 MHz, 288 MHz, 384 MHz, 576 MHz, **624 MHz**]
GT PM Support>	GT PM Support [**Enabled**, Disabled]
PAVP Enable>	PAVP [**Enabled**, Disabled]
BIA>	Auto: GMCH uses VBIOS default Level n: is enabled with selected aggressiveness level [**Auto**, Disabled, Level 1, Level 2, Level 3, Level 4, Level5]
ALS Support>	Valid only for ACPI [**Enable**, Disable]

Function	Second level Sub-Screen / Description
IGD Flat Panel>	[**Auto**, 640x480, 800x600, 1024x768, 1280x1024, 1366x768, 1680x1050, 1920x1200, 1280x800]
IGD Boot Type>	Select preference for IGD display interface used when system boots. [**Auto**, VGA port, HDMI, DP Port B, Dp Port C, eDP, DSI Prt A, DSI Port C]
Panel Scaling>	Sets Panel scaling [**Auto**, Centering, Stretching]
GMCH BLC Control>	Backlight control settings [**PWM-Inverted**, GMBus-Inverted, PWM-Normal, GMBus-Normal]
IPU Enable/Disable>	IPU Device [Enable, **Disable**]

10.2.3.4. Chipset> South Cluster Configuration

Figure 18: Chipset>South Cluster Configuration Menu Initial Screen Example



```
Aptio Setup Utility – Copyright (C) 2017 American Megatrends, Inc.
Chipset

▶ HD-Audio Configuration                    HD-Audio Configuration Settings
▶ LPSS Configuration
▶ PCI Express Configuration
▶ SATA Drives
▶ SCC Configuration
▶ USB Configuration
▶ Miscellaneous Configuration
                                            →←: Select Screen
                                            ↑↓: Select Item
                                            Enter: Select
                                            +/-: Change Opt.
                                            F1: General Help
                                            F2: Previous Values
                                            F3: Optimized Defaults
                                            F4: Save & Exit
                                            ESC: Exit

Version 2.18.1263. Copyright (C) 2017 American Megatrends, Inc.
```

The following table shows the South Cluster Configuration sub-screens and functions and describes the content. Default settings are in **bold** and for some functions, additional information is included.

The BIOS features in this user guide are open to change and may not be the latest version. The latest version may have differences to the options and features described in Table 23.

Table 23: Chipset>South Cluster Configuration Sub-screens and Functions

Function	Second level Sub-Screen / Description	
HD Audio Configuration>	HD-Audio Support>	HD-Audio support [**Enable**, Disable]
	HD-Audio DSP>	HD-Audio DSP [**Enable**, Disable]
	Audio DSP Feature Support:	
	Audio DSP Compliance Mode>	Sets DSP enabled system compliance: 1: Non-UAA (IntelSST driver support only – CC_040100) 2: UAA (HD Audio Inbox or IntelSST driver support – CC_040380) Note: NHLT (DMIC/BT/I2S configuration) is published for non-UAA only. [Non_UAA (IntelSST), **UAA (HD Inbox/IntelSST)**]
	WoV (Wake on Voice) >	DSP Feature. Bitmask structure: [BIT0] – WoV [BIT1] – BT Sideband [BIT2] – Codec based VAD [BIT3] – SRAM Reclaim [BIT5] – BT Intel HFP

Function	Second level Sub-Screen / Description	
HD Audio Configuration> (continued)	WoV (Wake on Voice) > (continued)	[BIT6] – BT Intel A2DP [BIT9] – Context Aware [Enabled, **Disabled**]
	Bluetooth Sideband>	DSP Feature. Bitmask structure: [BIT0] – WoV [BIT1] – BT Sideband [BIT2] – Codec based VAD [BIT3] – SRAM Reclaim [BIT5] – BT Intel HFP [BIT6] – BT Intel A2DP [BIT9] – Context Aware [**Enabled**, Disabled]
	SRAM Reclaim>	DSP Feature. Bitmask structure: [BIT0] – WoV [BIT1] – BT Sideband [BIT2] – Codec based VAD [BIT3] – SRAM Reclaim [BIT5] – BT Intel HFP [BIT6] – BT Intel A2DP [BIT9] – Context Aware [**Enabled**, Disabled]
	BT Intel HFP>	DSP Feature./ Bitmask structure: [BIT0] – WoV [BIT1] – BT Sideband [BIT2] – Codec based VAD [BIT3] – SRAM Reclaim [BIT5] – BT Intel HFP [BIT6] – BT Intel A2DP [BIT9] – Context Aware [**Enabled**, Disabled] [**Enabled**, Disabled]
	BT Intel A2DP>	DSP Feature. Bitmask structure: [BIT0] – WoV [BIT1] – BT Sideband [BIT2] – Codec based VAD [BIT3] – SRAM Reclaim [BIT5] – BT Intel HFP [BIT6] – BT Intel A2DP [BIT9] – Context Aware [Enabled, **Disabled**]
	Context Aware>	DSP Feature. Bitmask structure: [BIT0] – WoV [BIT1] – BT Sideband

Function	Second level Sub-Screen / Description	
HD Audio Configuration> (continued)	Context Aware> (continued)	[BIT2] – Codec based VAD [BIT3] – SRAM Reclaim [BIT5] – BT Intel HFP [BIT6] – BT Intel A2DP [Enabled, **Disabled**]
	NHLT Endpoints Configuration:	
	DMIC>	Selects DMIC to expose in NHLT ACPI table [2 Mic Array, 4 Mic Array, **Disabled**]
	Bluetooth>	Enables/Disables Bluetooth Endpoint in NHLT ACPI table [Enabled, **Disabled**]
	I2S SKP>	Read only, **Enabled**
	I2S HP>	Read only, **Enabled**
	Codex based VAD>	DSP Feature. Bitmask structure: [BIT0] – WoV [BIT1] – BT Sideband [BIT2] – Codec based VAD [BIT3] – SRAM Reclaim [BIT5] – BT Intel HFP [BIT6] – BT Intel A2DP [BIT9] – Context Aware [Enabled, **Disabled**]
	DSP based Speech Pre-Processing>	DSP Feature. Bitmask structure: [BIT0] – WoV [BIT1] – BT Sideband [BIT2] – Codec based VAD [BIT3] – SRAM Reclaim [BIT5] – BT Intel HFP [BIT6] – BT Intel A2DP [BIT9] – Context Aware [Enabled, **Disabled**]
	Voice Activity Detection>	Read only, **Intel Wake On Voice**
	Post-Processing Module Support:	
	Waves>	Enables/Disables 3rd Party Processing Module Support (identlfied by GUID). WoV must be enabled as a feature first to selecr relevent WoV IP. [Enabled, **Disabled**]
	DTS>	
	Spatial>	
	Dolby>	
	Samsung SoundAlive>	
	Samsung SoundBooster>	

Function	Second level Sub-Screen / Description	
HD Audio Configuration> (continued)	Samsung EQ/DRC>	Enables/Disables 3rd Party Processing Module Support (identlfied by GUID). WoV must be enabled as a feature first to selecr relevent WoV IP. [Enabled, **Disabled**]
	ForteMedia SAMSoft>	
	Intel WoV>	Read only, **Disabled**
	Sensory WoV>	Read only, **Disabled**
	Conexant Pre-Process>	Enables/Disables 3rd Party Processing Module Support (identlfied by GUID). WoV must be enabled as a feature first to selecr relevent WoV IP. [Enabled, **Disabled**]
	Context Aware Pre-Process>	
	Custom Module ‘Alpha‘>	
	Custom Module ‘Beta‘>	
	Custom Module ‘Gamma‘>	
	HD-Audio CSME Memory Transfers>	Sets HD-Audio CSME memory transfers to VC0/VC2 [**VC0**, VC2]
	HD-Audio Host Memory Transfers>	Sets HD-Audio Host memory transfers to VC0/VC2 [**VC0**, VC2]
	HD-Audio I/O Buffer Ownership Select>	Sets HD-Audio I/O buffer ownership [**HD-Audio link owns all the I/O buffers**, I2S port owns all the I/O buffers]
	HD-Audio Clock Gating>	HD-Audio Clock gating [**Enabled**, Disabled]
	HD-Audio Power Gating>	HD-Audio Power gating [**Enabled**, Disabled]
	HD-Audio PME>	HD-Audio PME [**Enabled**, Disabled]
	HD-Audio Link Frequency>	Selects HD-Audio link frequency Applicable only if HDA codec supports selected frequency. [6 MHz, 12 MHz, **24 MHz**]
	iDisplay Link Frequency>	Selects iDisplay Link frequency Applicable only if iDisp codec supports selected frequency. [48 MHz, **96 MHz**]
LPSS Configuration>	LPSS I2C1 Support (D22:F1)>	LPSS I2C1 Support (I2C_CAM0) [**Enable**, Disable]
	LPSS I2C2 Support (D22:F2)>	LPSS I2C2 Support (I2C_CAM1) [**Enable**, Disable]
	LPSS I2C3 Support (D22:F3)>	LPSS I2C3 Support (I2C_GP) [**Enable**, Disable]
	LPSS I2C4 Support (D22:F0)>	LPSS I2C4 Support (I2C_LCD) [**Enable**, Disable]

Function	Second level Sub-Screen / Description		
LPSS Configuration> (continued)	LPSS HSUART1 Support (D24:F1)>	LPSS HSUART1 Support [**Enable**, Disable]	
	LPSS HSUART2 Support (D24:F2)>	LPSS HSUART2 Support [**Enable**, Disable]	
	LPSS SPI0 Support (D25:F0)>	LPSS SPI0 Support [**Enable**, Disable]	
	LPSS IOSF PMCTL S0ix Enable>	LPSS IOSF Bridge PMCTL Register S0ix Bits [**Enable**, Disable]	
PCI Express Configuration>	PCI Express Clock Gating>	PCI Express clock gating for each root port [**Enabled**, Disabled]	
	Port8xh Decode>	PCI express port 8xh decode [Enabled, **Disabled**]	
	Peer Memory Write Enable>	Peer memory write [Enabled, **Disabled**]	
	Compliance Test Mode>	Enable when using compliance load board [Enabled, **Disabled**]	
	PCI Root Port 4 (GbE)> or PCI Root Port 5 (NC) or PCI Root Port 0 (QSEVEN PCIe#0)> or PCI Root Port 1 (QSEVEN PCIe#1)> or PCI Root Port 2 (QSEVEN PCIe#2)> or PCI Root Port 3 (QSEVEN PCIe#3)>	PCI Express Root Port[#]>	Controls the PCI Express port Auto automatically disables the unused root port for optimum power saving. [**Auto**,Enabled, Disabled]
		ASPM>	Active State Power Management (ASPM) level settings [**Disabled**, Auto, L0s, L1, L0sL1]
		L1 Substates>	PCI Express L1 substrates settings [Disabled, L1.1, L1.2, **L1.1 & L1.2**]
		ACS>	Access Control Service Extended Capability [**Enabled**, Disabled]
		URR>	PCI Express unsupported request reporting [Enabled, **Disabled**]
		FER>	PCI Express device fatal error reporting [Enabled, **Disabled**]
		NFER>	PCI Express device non-fatal error reporting [Enabled, **Disabled**]
		CER>	PCI Express device correctable error reporting [Enabled, **Disabled**]
		CTO>	PCI Express completion timer (T0) [**Default Setting**, 16-55 ms, 65-210 ms, 260-900 ms, 1-3.5 s, Disabled]
		SEFE>	Root PCI Express System Error on Fatal Error [Enabled, **Disabled**]
		SENFE>	Root PCI Express System Error on non-Fatal Error [Enabled, **Disabled**]

Function	Second level Sub-Screen / Description		
PCI Express Configuration> (continued)	PCI Root Port 4 (GbE)> or PCI Root Port 5 (NC) or PCI Root Port 0 (QSEVEN PCIe#0)> or PCI Root Port 1 (QSEVEN PCIe#1)> or PCI Root Port 2 (QSEVEN PCIe#2)> or PCI Root Port 3 (QSEVEN PCIe#3)> (continued)	SECE>	Root PCI Express System Error on correctable error [Enabled, **Disabled**]
		PME SCI>	PCI Express PME SCI [**Enabled**, Disabled]
		Hot Plug>	PCI Express hot plug [Enabled, **Disabled**]
		PCIe Speed>	Configures PCIe speed [**Auto**, Gen 1, Gen2]
		Transmitter Half Swing>	Transmitter half swing [Enabled, **Disabled**]
		Extra Bus Reserved>	Extra bus reserved for bridges behind this root bridge. (0-7)
		Reserved Memory>	Reserved memory and prefetchable memory for this root bridge Range: (1 MB-20 MB)
		Reserved I/O>	Reserved I/O for this root bridge Range: (**4** k, 8 k, 12 k, 16 k, 20 k)
		PCH PCIE LTR>	PCH PCIE latency reporting [**Enabled**, Disabled]
		Snoop Latency Override>	Snoop latency override or Non Snoop override for PCH PCIE. Disabled: disables override Manual: manually enters override values Auto: maintains default BIOS flow. [Disabled, Manual, **Auto**]
		Non Snoop Latency Override>	
		PCIE1 LTR Lock>	PCIE LTR configuration lock [Enabled, **Disabled**]
		PCIE Selectable De-emphasis>	Selects level of de-emphasis for an upstream component, if the Link operates at 5.0 GT/s speed. 1b – 3.5 dB 0b – 6 dB [**Enabled,** Disabled]
SATA Drivers>	SATA Test Mode>	Test mode [Enabled, **Disabled**]	
	SATA Port 0> or SATA Port 1>	SATA Port #>	Read only field SATA port installed/Not Installed and software preserve
		Port #>	SATA port # [**Enabled,** Disabled]

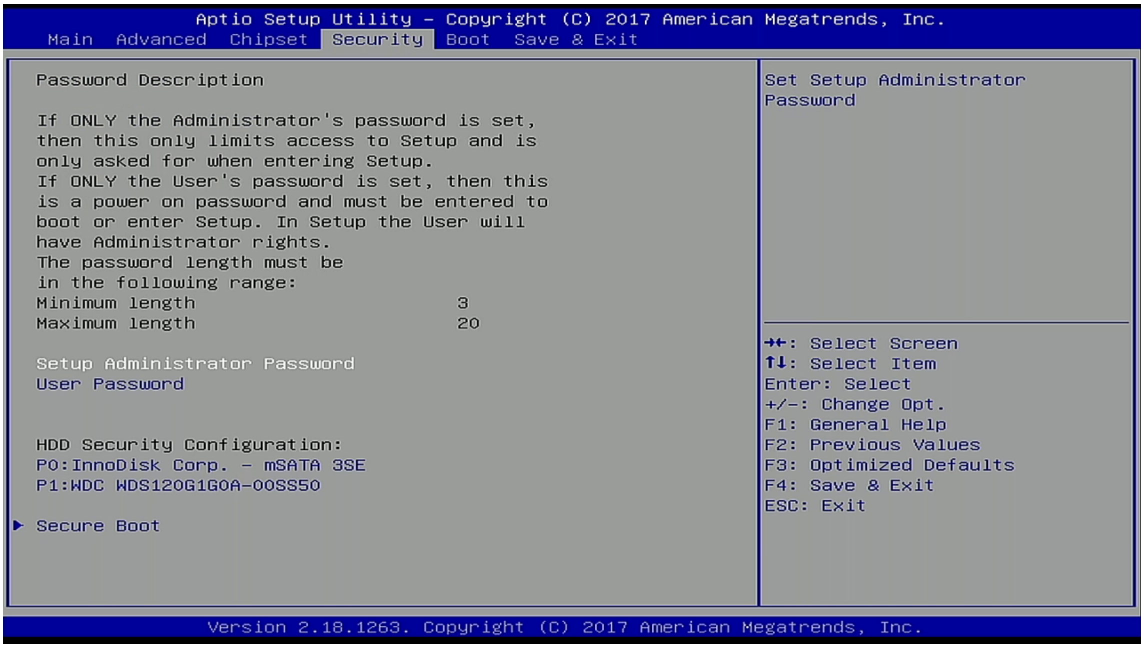
Function	Second level Sub-Screen / Description		
SATA Drivers> (continued)	SATA Port 0> or SATA Port 1> (continued)	SATA Port # Hot Plug Capability>	Reports SATA port as being Hot Plug capable [Enabled, **Disabled]**
SCC Configuration>	SCC SD Card Support (D27:F0)>	SCC card support [**Enabled**, Disabled]	
	SCC eMMC Support (D28:F0)>	SCC eMMC Support [**Enabled**, Disabled]	
	eMMC Max Speed>	Selects the eMMC max. speed allowed [HS400, **HS200**, DDR50]	
USB Configuration>	USB Port Disable Override>	Selectively enables or disables the corresponding USB port from reporting a device connection to the controller. [Enable, **Disable**]	
	xDCI Support>	XDCI [Enable, **Disable**]	
	xHCI Disable Compliance Mode>	xHCI Disable Compliance Mode [FALSE, TRUE]	
	USB HW Mode AFE Comparators>	USB HW mode AFE comparators [Enabled, **Disabled**]	
Miscellaneous Configuration>	State After G3>	Specifies the state to go to if power is reapplied after power failure (G3 state) S0 state: system boots directly as soon as power is applied. S5 state: system remains in power-off states until the power button is pressed. [**S0 State**, S5 State]	
	Power Button Debounce Mode>	Enable interrupt when PWRBTN# is asserted [**Enable**, Disable]	
	Wake On LAN>	Wake on LAN [Enable, **Disable**]	
	BIOS Lock>	Enable/Disable the SC BIOS Lock Enable feature. Required to be enabled to ensure SMM protection of flash [Enabled, **Disabled**]	
	RTC Lock>	Enable will lock bytes 38h-3Fh in the lower/upper 128-byte bank of RTC RAM [**Enabled**, Disabled]	
	TCO Lock>	Enable TCO and Lock Down TCO [Enabled, **Disabled**]	
	DCI Enable (HDCIEN)>	If enabled the user is considered to have consented to enable DCI and allows debug over the USB 3 interface. If disabled, the host controller does not enable the DCI feature. [Enabled, **Disabled**]	

Function	Second level Sub-Screen / Description	
Miscellaneous Configuration> (continued)	DCI Auto Detect Enable>	If set, DCI Auto detects if DCI is connected during BIOS post time and enables DCI. If not set, DCI is disabled. [**Enabled**, Disabled]
	GPIO Lock>	Enable to set GPIO Pad Configuration Lock for security [Enabled, **Disabled**]

10.2.4. Security Setup Menu

The Security setup menu provides information about the passwords and functions for specifying the security settings such as Hard Disk user and master passwords.

Figure 19: Security Setup Menu Initial Screen Example



```
          Aptio Setup Utility – Copyright (C) 2017 American Megatrends, Inc.
    Main  Advanced  Chipset  Security  Boot  Save & Exit

  Password Description                              Set Setup Administrator
                                                    Password
  If ONLY the Administrator's password is set,
  then this only limits access to Setup and is
  only asked for when entering Setup.
  If ONLY the User's password is set, then this
  is a power on password and must be entered to
  boot or enter Setup. In Setup the User will
  have Administrator rights.
  The password length must be
  in the following range:
  Minimum length                      3
  Maximum length                      20
                                                    →←: Select Screen
  Setup Administrator Password                      ↑↓: Select Item
  User Password                                     Enter: Select
                                                    +/-: Change Opt.
                                                    F1: General Help
  HDD Security Configuration:                       F2: Previous Values
  P0:InnoDisk Corp. - mSATA 3SE                     F3: Optimized Defaults
  P1:WDC WDS120G1G0A-00SS50                         F4: Save & Exit
                                                    ESC: Exit
▶ Secure Boot

          Version 2.18.1263. Copyright (C) 2017 American Megatrends, Inc.
```

The following table shows the Security sub-screens and functions and describes the content. Default settings are in **bold** and for some functions, additional information is included.

The BIOS features in this user guide are open to change and may not be the latest version. The latest version may have differences to the options and features described in Table 24.

Table 24: Security Setup Menu Initial Screen

Function	Description
Setup Administrator Password>	Sets administrator password
User Password>	Sets user password
HDD Security Configuration>	Read Only Information Allows access to set, modify and clear Hard Disk user and master passwords. User Passwords need to be installed for Enabling Security. Master Password can be modified only when successfully unlocked with the Master Password in Post. If the 'Set HDD Password' is grayed out, then power cycle to enable the option again. HDD Password Configuration Security supported : Yes Security Enabled : No Security Locked : No

Function	Description		
HDD Security Configuration (continued)	Security Frozen : No HDD User Pwd Status : Not Installed HDD Master Pwd Status : Installed		
	Set User Password>	Sets HDD password. Note: It is advisable to power cycle the system after setting Hard Disk passwords. The 'Discarding or Saving Changes' in the setup does not have an impact on HDD when the password is set or removed. If the setup HDD user Password is grayed out, do power cycle enable the option again.	
Secure Boot>	System Mode>	Read only information.	
	Secure Boot>		
	Vendor Keys>		
	Attempt Secure Boot>	Secure Boot activated when Platform Key (PK) is enrolled, System mode is User/Deployed, and CSM function is disabled [Enabled, **Disabled**]	
	Secure Boot Mode>	Set UEFI Secure Boot Mode to STANDARD mode or CUSTOM mode [Standard, **Customized**]	
	Key Management>	Enables expert users to modify Secure Boot Policy variables without full authentication	
		Provision Factory Default keys>	Allow to provision factory default Secure Boot keys when System is in Setup Mode [Enabled, **Disabled**]
		Install Factory Default keys>	Force System to User Mode – install all Factory Default keys
		Enroll Efi Image>	Allow the image to run in Secure Boot mode. Enroll SHA256 Hash Certificate of the Image into Authorized Signature Database (db)
		Platform Key (PK)>	Enroll Factory Defaults or load certificates from a file: Public Key Certicate in: EFI_SIGNATURE_LIST EFI_CERT_X509 (DER encoded) EFI_CERT_RSA2048 (bin) EFI_CERT_SHA256,385,512 Authenticated UEFI Variable EFI PE/COFF Image (SHA256) Key Source : Default, External, Mixed, test
		Key Exchange Keys>	
		Authorized Signatures>	
		Forbidden Signatures>	
		Authorized TimeStamps>	
		OsRecovery Signatures>	

10.2.4.1. Remember the Password

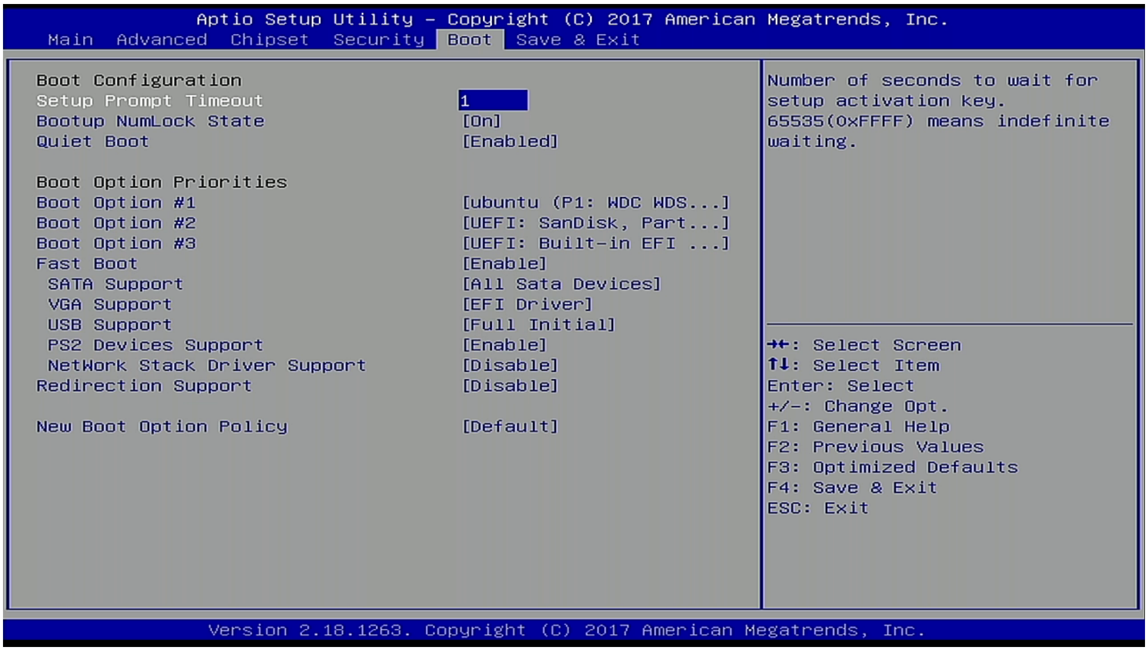
It is recommended to keep a record of all passwords in a safe place. Forgotten passwords results in the user being locked out of the system. If the system cannot be booted because the User Password or the Supervisor Password are not known, clear the uEFI BIOS settings, or contact Kontron Support for further assistance.

HDD security passwords cannot be cleared using the above method.

10.2.5. Boot Setup Menu

The Boot setup menu lists the dynamically generated boot-device priority order.

Figure 20: Boot Setup Menu Initial Screen Example



```
        Aptio Setup Utility – Copyright (C) 2017 American Megatrends, Inc.
  Main  Advanced  Chipset  Security  Boot  Save & Exit

  Boot Configuration                                       Number of seconds to wait for
  Setup Prompt Timeout                    1                setup activation key.
  Bootup NumLock State                    [On]             65535(0xFFFF) means indefinite
  Quiet Boot                              [Enabled]        waiting.

  Boot Option Priorities
  Boot Option #1                          [ubuntu (P1: WDC WDS...]
  Boot Option #2                          [UEFI: SanDisk, Part...]
  Boot Option #3                          [UEFI: Built-in EFI ...]
  Fast Boot                               [Enable]
   SATA Support                           [All Sata Devices]
   VGA Support                            [EFI Driver]
   USB Support                            [Full Initial]
   PS2 Devices Support                    [Enable]         →←: Select Screen
   NetWork Stack Driver Support           [Disable]        ↑↓: Select Item
  Redirection Support                     [Disable]        Enter: Select
                                                           +/-: Change Opt.
  New Boot Option Policy                  [Default]        F1: General Help
                                                           F2: Previous Values
                                                           F3: Optimized Defaults
                                                           F4: Save & Exit
                                                           ESC: Exit

        Version 2.18.1263. Copyright (C) 2017 American Megatrends, Inc.
```

The following table shows the Boot set up sub-screens and functions and describes the content. Default settings are in bold.

The BIOS features in this user guide are open to change and may not be the latest version. The latest version may have differences to the options and features described in Table 25.

Table 25: Boot Setup Menu Sub-screens and Functions

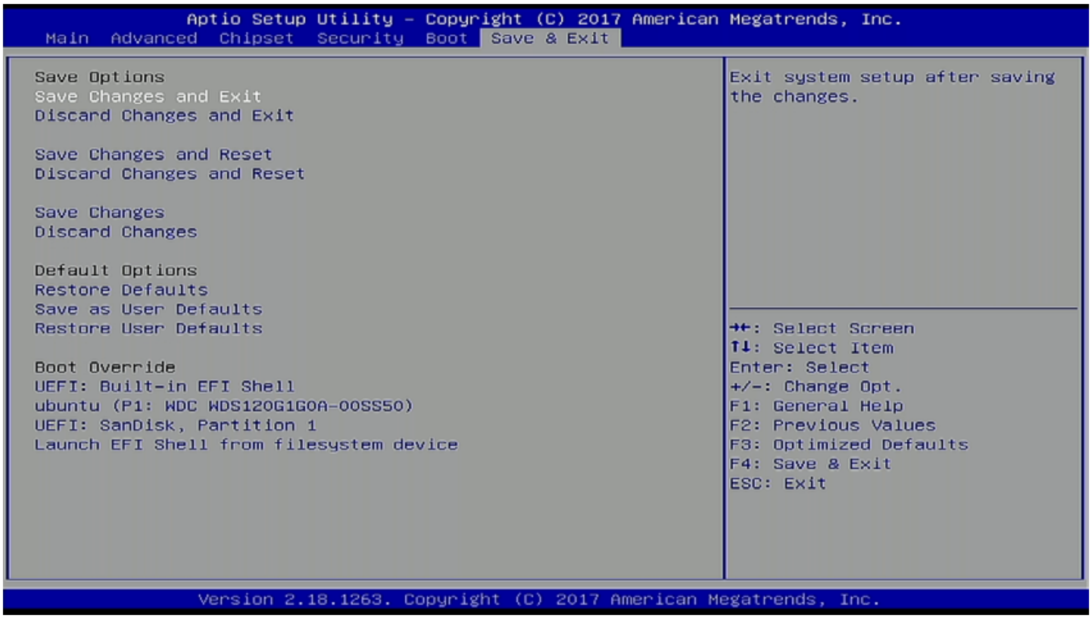
Function	Description
Setup Prompt Timeout>	Displays number of seconds that the firmware waits for setup activation key The value 65535(0xFFFF) means an indefinite wait.
Bootup NumLock State>	Selects keyboard NumLock state [**ON**, OFF]
Quiet Boot>	Quiet Boot [Enabled, **Disabled**]
Boot Option #>	Sets the system boot order
Fast Boot>	Enables or disables FastBoot features Note: Most probes are skipped to reduce time and cost during boot. [Enabled, **Disabled**]
SATA Support>	SATA Support [Last Boot HDD only, **All Sata Devices**]

Function	Description
VGA Support>	If Auto, only install Legacy OpRom with Legacy OS and logo would NOT be shown during post. Efi driver will still be installed with EFI OS. [Auto, **EFI Driver**]
USB Support>	If disabled, all USB devices will NOT be available untill after OS boot. If Partial Initial, USB Mass Storage and specific USB port/device will NOT be available before OS boot. If Full Initial, all USB devices will be available in OS and Post. [**Full Initial**, Partial Initial, Disable]
PS2 Support>	PS2 Support [**Enabled**, Disabled]
Netwrok Stack Driver Support>	Netwrok Stack Driver Support [Enabled, **Disabled**]
Redirection Support>	Redirection Support [Enabled, **Disabled**]
New Boot Option Policy>	Controls the placement of newly detected UEFI boot options [**Default**, Place First, Place Last]

10.2.6. Save and Exit Setup Menu

The Save and Exit setup menu provides functions for handling changes made to the settings and exiting the program.

Figure 21: Save and Exit Setup Menu Initial Screen Example



```
          Aptio Setup Utility – Copyright (C) 2017 American Megatrends, Inc.
   Main  Advanced  Chipset  Security  Boot  Save & Exit

  Save Options                                          Exit system setup after saving
  Save Changes and Exit                                 the changes.
  Discard Changes and Exit

  Save Changes and Reset
  Discard Changes and Reset

  Save Changes
  Discard Changes

  Default Options
  Restore Defaults
  Save as User Defaults
  Restore User Defaults                                 →←: Select Screen
                                                        ↑↓: Select Item
  Boot Override                                         Enter: Select
  UEFI: Built-in EFI Shell                              +/-: Change Opt.
  ubuntu (P1: WDC WDS120G1G0A-00SS50)                   F1: General Help
  UEFI: SanDisk, Partition 1                            F2: Previous Values
  Launch EFI Shell from filesystem device               F3: Optimized Defaults
                                                        F4: Save & Exit
                                                        ESC: Exit

            Version 2.18.1263. Copyright (C) 2017 American Megatrends, Inc.
```

The following table shows the Save and Exit sub-screens and functions and describes the content.

The BIOS features in this user guide are open to change and may not be the latest version. The latest version may have differences to the options and features described in Table 26.

Table 26: Save and Exit Setup Menu Sub-screens and Functions

Function	Description
Save Changes and Exit >	Exits system after saving changes
Discard Changes and Exit>	Exits system setup without saving changes
Save Changes and Reset>	Resets system after saving changes
Discard Changes and Reset>	Resets system setup without saving changes
Save Changes>	Saves changes made so far for any setup options
Discard Changes>	Discards changes made so far for any setup options
Restore Defaults>	Restores/loads standard default values for all setup options
Save as User Defaults>	Saves changes made so far as user defaults
Restore User Defaults>	Restores user defaults to all setup options
UEFI: Built in EFI Shell>	Attempts to launch the boot option #1
Ubuntu (P1: WDC WDS120G1G0A-00SS50)>	Attempts to launch the boot option #2
UEFI: SanDisk, Partition 1>	Attempts to launch the boot option #3
Launch EFI Shell from File System Device>	Attempts to launch EFI Shell application (Shell.efi) from one of the available file system devices

10.3. The uEFI Shell

The Kontron uEFI BIOS features a built-in and enhanced version of the uEFI Shell. For a detailed description of the available standard shell scripting, refer to the EFI Shell User Guide. For a detailed description of the available standard shell commands, refer to the EFI Shell Command Manual. Both documents can be downloaded from the EFI and Framework Open Source Community homepage (http://sourceforge.net/projects/efi-shell/files/documents/).

AMI APTIO update utilities for DOS, EFI Shell and Windows are available at AMI.com: http://www.ami.com/support/downloads/amiflash.zip.

Kontron uEFI BIOS does not provide all shell commands described in the EFI Shell Command Manual.

10.3.1. Basic Operation of the uEFI Shell

The uEFI Shell forms an entry into the uEFI boot order and is the first boot option by default.

10.3.1.1. Entering the uEFI Shell

To enter the uEFI Shell, follow the steps below:

1. Power on the module, see Chapter 9/Power on.
2. Press the <F7> key (instead of <DEL>) to display a choice of boot devices.
3. Choose 'UEFI: Built-in EFI shell'.

```
EFI Shell version 2.40 [5.11]
Current running mode 1.1.2
Device mapping table
Fs0        :HardDisk - Alias hd33b0b0b fs0
  Acpi(PNP0A03,0)/Pci(1D|7)/Usb(1, 0)/Usb(1, 0)/HD(Part1,Sig17731773)
```

4. Press the <ESC> key within 5 seconds to skip startup.nsh, and any other key to continue.
5. The output produced by the device-mapping table can vary depending on the board's configuration.
6. If the <ESC> key is pressed before the 5 second timeout elapses, the shell prompt is shown:

```
Shell>
```

10.3.1.2. Exiting the uEFI Shell

To exit the uEFI Shell, follow one of the steps below:

1. Use the **exit** uEFI Shell command to select the boot device, in the Boot menu, that the OS boots from.
2. Reset the board using the **reset** uEFI Shell command.

10.4. uEFI Shell Scripting

10.4.1. Startup Scripting

If the <ESC> key is not pressed and the timeout has run out then the uEFI Shell automatically tries to execute some startup scripts. It searches for scripts and executes them in the following order:

1. Initially searches for Kontron flash-stored startup script.
2. If there is no Kontron flash-stored startup script present, then the uEFI-specified **startup.nsh** script is used. This script must be located on the root of any of the attached FAT formatted disk drive.
3. If none of the startup scripts are present or the startup script terminates then the default boot order is continued.

10.4.2. Create a Startup Script

Startup scripts can be created using the uEFI Shell built-in editor **edit** or under any OS with a plain text editor of your choice. To create a startup shell script, simply save the script on the root of any FAT-formatted drive attached to the system. To copy the startup script to the flash, use the **kBootScript** uEFI Shell command.

In case there is no mass storage device attached, the startup script can be generated in a RAM disk and stored in the SPI boot flash using the **kRamdisk** uEFI Shell command.

10.4.3. Example of Startup Scripts

10.4.3.1. Execute Shell Script on other Harddrive

This example (**startup.nsh)** executes the shell script named **bootme.nsh** located in the root of the first detected disc drive (**fs0**).

```
fs0:
bootme.nsh
```

10.5. Firmware Update

Firmware updates are typically delivered as a ZIP archive containing only the firmware images. The content of the archive with the directory structure must be copied onto a data storage device with FAT partition.

10.5.1. Updating Procedure

BIOS can be updated with the Intel tool fpt.efi using the procedure below:

1. Copy these files to an USB stick.
   - flash.nsh (if available)
   - fpt.efi
   - fparts.txt
   - Q7ALx2i<xxx>.bin (where xxx stands for the version #)
   - Start the system into setup.

2. Change the following setup items:

   Chipset > South Cluster Configuration> Miscellaneous Configuration > BIOS Lock > Disabled

3. Save and Exit the BIOS setup.

Changes are only effective during the first boot after applying the change. Failing to flash during the next boot, may require steps 3 to be repeated.

4. On the next start, boot into shell.

5. Change to the drive representing the USB stick.

   ```
   fsx:   (x = 0,1,2,etc. represents the USB stick)
   ```

   Change to the directory where you copied the flash tool.

   ```
   cd <your_directory>
   ```

6. Start flash.nsh (if available) OR enter

   ```
   fpt  –F Q7ALx2i<xxx>.bin
   ```

7. Wait until flashing is successful and then power cycle the board.

Do not switch off the power during the flash process!
Doing so leaves your module unrecoverable.

Appendix A: List of Acronyms

Table 27: List of Acronyms

ACPI	Advanced Configuration and Power Interface
BIOS	Basic Input Output System
CAN	Controller-area network
Carrier Board	Application specific circuit board that accepts a COM Express ® module
CEC	Consumer Electronics Control
CPLD	Complex Programmable Logic Devices
DDC	Display Data Control
DDI	Digital Display Interface
DDIO	Digital Display Input/Output
DMA	Direct Memory Access
DP	DisplayPort (digital display interface standard)
DRAM	Dynamic Random Access Memory
DVI	Digital Visual Interface
ECC	Error Checking and Correction
EEPROM	Electrically Erasable Programmable Read-Only Memory
eDP	Embedded Display Port
EMC	Electromagnetic Compatibility
eMMC	embedded MultiMedia flash Card
ESD	Electro Sensitive Device
FAT	File Allocation Table
FIFO	First In First Out
Gb	Gigabit
GBE	Gigabit Ethernet
GPI	General Purpose Input
GPIO	General Purpose Input Output
GPO	General Purpose Output
GPU	Graphics Processing Unit
HBR2	High Bitrate 2
HDA	High Definition Audio (HD Audio)
HD/HDD	Hard Disk /Drive
HDMI	High Definition Multimedia Interface
HWM	Hardware Monitor
I2C	Inter integrated Circuit Communications
I2S	Inter-IC Sound
IOT	Internet of Things
JTAG	Joint Test Action Group
LAN	Local Area Network
LPC	Low Pin-Count Interface:
LPT	Line Printing Terminal
LSB	Least Significant Bit
LVDS	Low Voltage Differential Signaling
MLC	Multi Level Cell
MTBF	Mean Time Before Failure
NA	Not Available
NC	Not Connected
NCSI2	Network Communications Services Interface
PCI	Peripheral Component Interface
PCIe	PCI-Express
PEG	PCI Express Graphics
PHY	Ethernet controller PHYsical layer
pMLC	Pseudo Multi Level Cell
pSLC	Pseudo Single Level Cell
PSU	Power Supply Unit
PWM	Pulse Width Modulation
RoHS	Restriction of the use of certain Hazardous Substances
RPM	Revolutions Per Minute
RTC	Real Time Clock
SATA	Serial AT Attachment:
SDIO	Secure Digital Input/Output
SLC	Single Level Cell
SoC	System on a Chip
SPI	Serial Peripheral Inteface
TPM	Trusted Platform Module
UART	Universal Asynchronous Receiver Transmitter
UEFI	Unified Extensible Firmware Interface
USB	Universal Serial Bus
VGA	Video Graphics Adapter
WDT	WatchDog Timer
WDOUT	WatchDog Time Out
WDTRIG	WatchDog TRigger
WEEE	Waste Electrical and Electronic Equipement (directive)

kontron
S&T Group

About Kontron

Kontron is a global leader in IoT/Embedded Computing Technology (ECT). As a part of technology group S&T, Kontron, together with its sister company S&T Technologies, offers a combined portfolio of secure hardware, middleware and services for Internet of Things (IoT) and Industry 4.0 applications. With its standard products and tailor-made solutions based on highly reliable state-of-the-art embedded technologies, Kontron provides secure and innovative applications for a variety of industries. As a result, customers benefit from accelerated time-to-market, reduced total cost of ownership, product longevity and the best fully integrated applications overall.

For more information, please visit: www.kontron.com

Global Headquarters

Kontron Europe GmbH

Gutenbergstraße 2
85737 Ismaning, Germany
Tel.: + 49 821 4086-0
Fax: + 49 821 4086-111
info@kontron.com