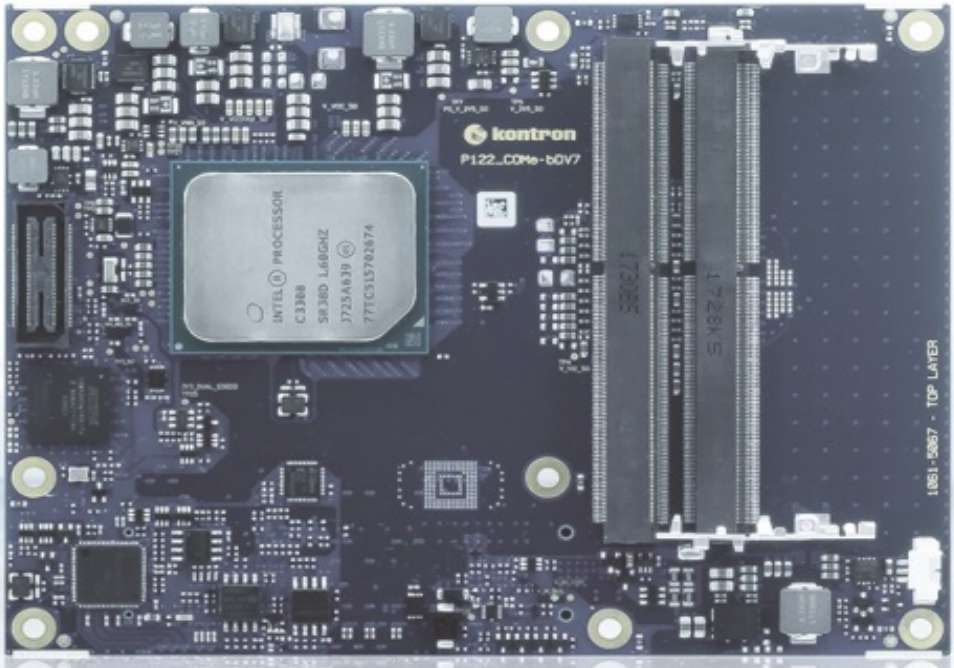
USER GUIDE



COMe-bDV7

Doc. User Guide, Rev 1.3

Doc. ID: 1062-0642

This page has been intentionally left blank

COME-BDV7 - 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 S&T AG

Lise-Meitner-Str. 3-5
86156 Augsburg
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/ Editor
1.0	Initial Version	2018-Oct-23	CW
1.1	Additions to Chapter 7, Standard and Certification and Chapter 11 connector pin assignment information.	2018-Nov-29	CW
1.2	Updates SLC information in Chapters 3.10 and 9.2	2019-Apr-01	CW
1.3	Added 32 GB memory, changed HSIO in processor tables, added QAT and VT as features.	2019-May-02	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.
	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.

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 become 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 COMe-bDV7 made by Kontron and focuses on describing the COMe-bDV7's special features. New users are recommended to study this user guide before switching on the power.

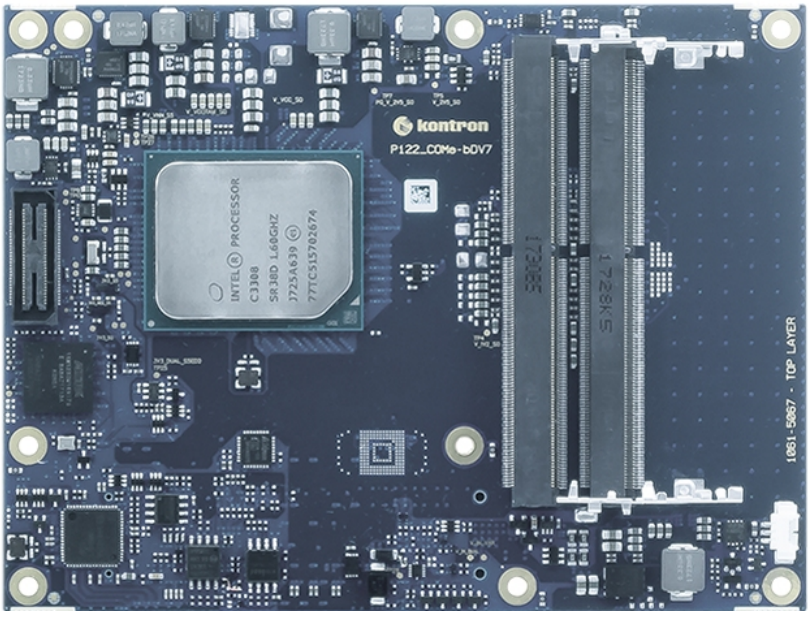
1.1. Product Description

The COMe-bDV7 is part of Kontron's COM Express® module family. The COMe-bDV7 is an entry level server-grade platform based on the Intel® Atom® C3000 SoC processor series featuring scalable CPU performance with up to 16 cores. This performance combined with quad 10GbE interfaces, and an additional Gigabit interface makes the COMe-bDV7 ideal for network intensive implementations.

General COMe-bDV7 features are:

- Entry level server-grade platform
- Quad 10 GbE and one Gigabit Ethernet
- High-speed connectivity PCIe 3.0, SATA3, USB 3.0
- 2x DDR4-2400 SODIMM sockets for up to 32 GB (non-ECC/ECC)
- Industrial grade version

Figure 1: COMe-bDV7 COM Express® Module



1.2. Product Naming Clarification

COM Express® defines a Computer-on-Module, or COM, with all the components necessary for a bootable host computer, packaged as a super component. The product names for Kontron COM Express® Computer-on-Modules consist of:

- Short form of the industry standard
  - COMe-
- Module form factor
  - b=basic (125mm x 95mm)
  - c=compact (95mm x 95mm)
  - m=mini (84mm x 55mm)
- Intel's® processor code name
  - DV = Denverton-NS
- Pinout type
  - Type 6
  - Type 7
  - Type10
- Available temperature variants
  - Commercial
  - Extended (E1)
  - Industrial (E2)
  - Screened industrial (E2S) and Rapid shutdown screened industrial (R E2S)
- Processor Identifier
- Chipset identifier (if chipset assembled)
- Memory size
  - Memory module (#G)/eMMC pSLC memory (#S)

1.3. COM Express® Documentation

The COM Express® specification defines the COM Express® module form factor, pinout and signals. The COM Express document is available on the PICMG® website.

1.4. COM Express® Functionality

All Kontron COM Express® basic and compact modules contain two 220-pin connectors. Each connector has two rows called Row A & B on the primary connector and Row C & D on the secondary connector. COM Express® Computer-on-Modules feature the following maximum amount of interfaces according to the PICMG module pinout type. Type 7 contains the Type 6 features with the exception of audio and video interfaces and with reduced SATA and USB interfaces.

Table 1: Pin Assignment of Type 6 and COMe-bDV7

Feature	Type 7 Pinout	COMe-bDV7 Pinout
Gigabit Ethernet	1x	1x
10 Gb Ethernet	4x	4x
NC-SI Interface	1x	1x
Serial ATA	2x	2x (Option to implement SATA1 as additional USB 3.0
PCI Express	32x	Up to 14 PCIe Gen3
USB Client	1x	
USB 3.0	4x	3x (Option to implement SATA1 as additional USB 3.0)
USB 2.0	4x	4x (Option3x UBS 2.0 with WIBU implemented on USB 2.0 port 3)
LPC	1x (or eSPI)	1x
External SMB	1x	1x
External I2C	1x	1x
GPIO	8x	8x
SDIO shared w/GPIO	1x	
UART (2-wire COM)	2x	2x
FAN PWM out	1x	1x

1.5. COM Express® Benefits

COM Express® defines a Computer-on-Module, or COM, with all the components necessary for a bootable host computer, packaged as a highly integrated computer. All Kontron COM Express® modules are very compact and feature a standardized form factor and a standardized connector layout that carry a specified set of signals. Each COM is based on the COM Express® specification. This standardization allows designers to create a single-system carrier board that can accept present and future COM Express® modules.

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

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

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

2/ Product Specification

2.1. Module Variants

The COMe-bDV7 is available in different processor, chipset and temperature variants to cover demands in performance, price and power.

2.2. Commercial Grade Modules (0°C to +60°C)

Table 2: Product Number for Commercial Grade Modules (0°C to +60°C operating)

Product Number	Product Name	Description
68006-0000-58-9	COMe-bDV7C3958	COM Express® basic pin-out type 7 Computer-on-Module with Intel® Atom® Processor C3958, 16 core, 2.0 GHz, 4x 10 GbE, 2x DDR4 SODIMM socket
68006-0000-58-8	COMe-bDV7C3858	COM Express® basic pin-out type 7 Computer-on-Module with Intel® Atom® Processor C3858, 12 core, 2.0 GHz, 4x 10 GbE, 2x DDR4 SODIMM socket
68006-0000-58-7	COMe-bDV7C3758	COM Express® basic pin-out type 7 Computer-on-Module with Intel® Atom® Processor C3758, 8 core, 2.2GHz, 4x 10 GbE, 2x DDR4 SODIMM socket
68006-0000-58-5	COMe-bDV7C3558	COM Express® basic pin-out type 7 Computer-on-Module with Intel® Atom® Processor C3558, 4 core, 2.2GHz, 2x 10 GbE + 2x 2.5 GbE, 2x DDR4 SODIMM socket

2.3. Industrial Temperature Grade Modules (E2, -40°C to +85°C)

Table 3: Product Number for Industrial Grade Modules (-40°C to +85°C operating)

Product Number	Product Name	Description
68007-0000-08-8	COMe-bDV7 E2 C3808	COM Express® basic pin-out type 7 Computer-on-Module with Intel® Atom® Processor C3808, 12 core, 2.0 GHz, 4x 10 GbE, 2x DDR4 SODIMM socket, Industrial temperature
68007-0000-08-7	COMe-bDV7 E2 C3708	COM Express® basic pin-out type 7 Computer-on-Module with Intel® Atom® Processor C3708, 8 core, 1.7 GHz, 4x 10 GbE, 2x DDR4 SODIMM socket, Industrial temperature
68007-0000-08-5	COMe-bDV7 E2 C3508	COM Express® basic pin-out type 7 Computer-on-Module with Intel® Atom® Processor C3508, 4 core, 1.5 GHz, 4x 2.5 GbE, 2x DDR4 SODIMM socket, Industrial temperature
68007-0000-08-3	COMe-bDV7 E2 C3308	COM Express® basic pin-out type 7 Computer-on-Module with Intel® Atom® Processor C3308, 2 core, 1.6 GHz, 4x 2.5 GbE, 1x DDR4 SODIMM socket, Industrial temperature

2.4. Rapid Shutdown Industrial Temperature Grade Modules (R E2, -40°C to +85°C)

Industrial temperature grade modules with rapid shutdown R E2 (-40°C to +85°C) are available by screening. For further information regarding the screening process, contact Kontron Support.

Kontron's rapid shutdown perfoms a controlled accelerated system shutdown. For more information, see Chapter9.8: Radid Shutdown.

2.5. Accessories

Accessories are either specific to the COMe-bDV7 or the COMe pin-out Type 7. For more information regarding accessories for your Kontron product, contact your local Kontron sales representative or Kontron Inside Sales.

Table 4: Product Accessories

Part Number		Description
68007-0000-00-0	HSP COMe-bDV7, thread	Heatspreader for COMe-bDV7 threaded mounting holes
38025-0000-99-0C05	HSK COMe-basic Active (w/o HSP)	Active Cooler for COMe-bxL6/bDV7 to be mounted on HSP
38025-0000-99-0C06	HSK COMe-basic passive (w/o HSP)	Passive Cooler for COMe-bxL6/bDV7 to be mounted on HSP

Table 5: COMe Pin-out Type 7 Accessories

Part Number	COMe Carrier	Description
68300-0000-00-0	COMe Eval Carrier Type 7	COM Express® Eval Carrier Type 7 Project Code: Topanga Canyon
68300-0000-01-0	ADA-COME-T7 4X10G RJ45	COMe Type 7 Interposer card, 4x 10 GbE RJ45 adapter to be used in combination with COMe Eval Carrier T7

Table 6: Memory Modules

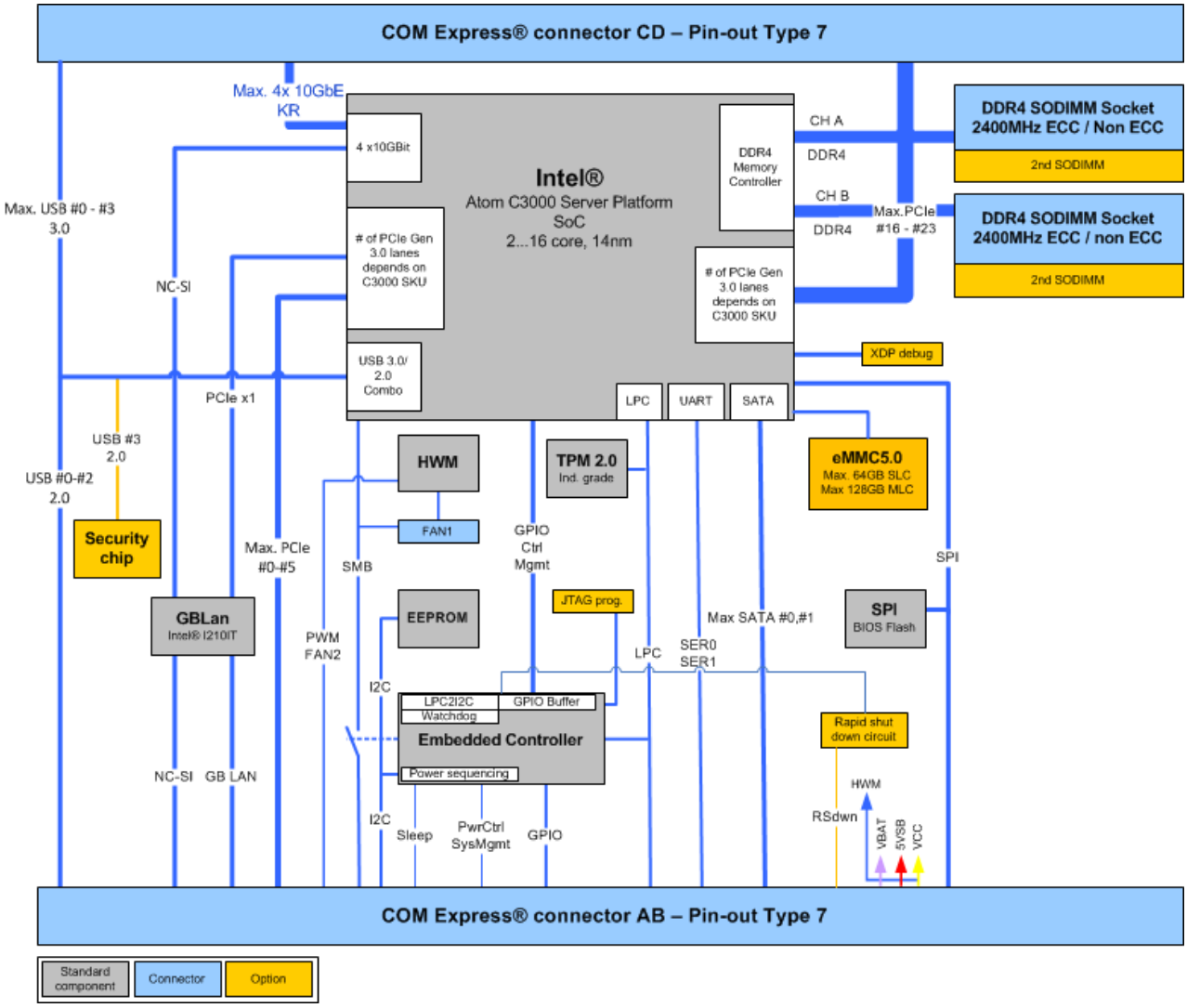
Part Number	Memory (Non ECC)	Description
97017-4096-24-0	DDR4-2400 SODIMM 4 GB_COM	DDR4-2400, 4 GB, 260P, 1200 MHz, PC4-2400 SODIMM
97017-8192-24-0	DDR4-2400 SODIMM 8 GB_COM	DDR4-2400, 8 GB, 260P, 1200 MHz, PC4-2400 SODIMM
97017-1600-24-0	DDR4-2400 SODIMM 16 GB_COM	DDR4-2400, 16 GB, 260P, 1200 MHz, PC4-2400 SODIMM
97017-3200-24-0	DDR4-2400 SODIMM 32 GB_COM	DDR4-2400, 32 GB, 260P, 1200 MHz, PC4-2400 SODIMM
97017-4096-24-2	DDR4-2400 SODIMM 4 GB E2_COM	DDR4-2400, 4 GB, E2, 260P, 1200 MHz, PC4-2400 SODIMM, industrial temperature
97017-8192-24-2	DDR4-2400 SODIMM 8 GB E2_COM	DDR4-2400, 8 GB, E2, 260P, 1200 MHz, PC4-2400 SODIMM, industrial temperature
97017-1600-24-2	DDR4-2400 SODIMM 16 GB E2_COM	DDR4-2400, 16 GB, E2, 260P, 1200 MHz, PC4-2400 SODIMM, industrial temperature
97017-3200-24-2	DDR4-2400 SODIMM 32 GB E2_COM	DDR4-2400, 32 GB, E2, 260P, 1200 MHz, PC4-2400 SODIMM, industrial temperature
Part Number	**Memory (ECC)**	**Description**
97018-4096-24-0	DDR4-2400 SODIMM 4 GB ECC_COM	DDR4-2400, 4 GB, ECC, 260P, 1200 MHz, PC4-2400 SODIMM

Part Number	Memory (Non ECC)	Description
97018-8192-24-0	DDR4-2400 SODIMM 8 GB ECC_COM	DDR4-2400, 8GB, ECC, 260P, 1200 MHz, PC4-2400 SODIMM
97018-1600-24-0	DDR4-2400 SODIMM 16 GB ECC_COM	DDR4-2400, 16 GB, ECC, 260P, 1200 MHz, PC4-2400 SODIMM
97018-3200-24-0	DDR4-2400 SODIMM 32 GB ECC_COM	DDR4-2400, 32 GB, ECC, 260P, 1200 MHz, PC4-2400 SODIMM
97018-4096-24-2	DDR4-2400 SODIMM 4 GB ECC E2_COM	DDR4-2400, 4 GB, ECC, E2, 260P, 1200 MHz, PC4-2400 SODIMM, industrial temperature
97018-8192-24-2	DDR4-2400 SODIMM 8 GB ECC E2_COM	DDR4-2400, 8 GB, ECC, E2, 260P, 1200 MHz, PC4-2400 SODIMM, industrial temperature
97018-1600-24-2	DDR4-2400 SODIMM 16 GB ECC E2_COM	DDR4-2400, 16 GB, ECC, E2, 260P, 1200 MHz, PC4-2400 SODIMM, industrial temperature
97018-3200-24-2	DDR4-2400 SODIMM 32 GB ECC E2_COM	DDR4-2400, 32 GB, ECC, E2, 260P, 1200 MHz, PC4-2400 SODIMM, industrial temperature

3/ Functional Specification

3.1. Block Diagram

Figure 2: Block Diagram COMe-bDV7



3.2. Processor

The Intel® Atom ® processor C3000 series, formerly Denverton-NS, uses the 14 nm processor technology with 34 mm x 28 mm package size and BGA 1310.

General Intel® Atom® C3000 Supported Technologies are:

- Intel® 64 Architecture
- Intel® Virtualization Technology (VT-x) and for Directed I/O (VT-d)
- Intel® VT-x with Extended Page Tables (EPT)
- Intel® Turbo Boost Technology
- Intel® Streaming SIMD Extensions 4.1 (Intel® SSE4.1)
- Intel® Streaming SIMD Extensions 4.1 (Intel® SSE4.1)
- Secure Hash Algorithm New Instruction (SHA-NI)
- Enhanced Intel SpeedStep® Technology
- Intel® AES New Instructions (AES-NI)
- Execute Disable Bit
- Quick Assist Technology

The Intel Atom® processor C3000 series offers scalable performance, configurable I/O ports and high performance Ethernet. The following table lists the processor specific specifications.

Table 7: Intel® Denverton-NS- Atom® Processor Specifications Commercial Temperature

Intel® Denverton Processor	Atom® C3958	Atom® C3858	Atom® C3758	Atom® C3558
# of Cores	16	12	8	4
# of Threads	16	12	8	4
# of HSIO Lanes	20[2]	20[2]	20[2]	12[2]
Processor Base Frequency	2 GHz	2 GHz	2.2 GHz	2.2 GHz
Max Turbo Frequency	2 GHz	2 GHz	2.2 GHz	2 GHz
TDP	31 W	25 W	25 W	16 W
Cache	16 MB	12 MB	8 MB	8 MB
Memory Types	DDR4-2400	DDR4-2400	DDR4-2400	DDR4-2133
Max.# Memory Channels	2	2	2	2
Max. Memory Size	256 GB[1]	256 GB[1]	256 GB[1]	256 GB[1]
ECC Memory	Yes	Yes	Yes	Yes
Integrated LAN	4x 10/2.5/1 GbE	4x 10/2.5/1 GbE	4x 10/2.5/1 GbE	2x 10/2.5/1 GbE + 2x 2.5/1 GbE
Intel®Quick Assist (QAT)	Supported			
QAT Speed	High	Medium	Low	Low
QAT Cryptographic Functions	Supported			
QAT Compression / Decompression	Supported			

[1] The COMe-bDV7 supports a max. of 128 GB with 4 SODIMM sockets /respect. 64 GB with 2-SODIMM sockets

[2] The HSIO lanes are shared and used for PCIe, USB3.0, SATA. Depending on the number of supported HSIO lanes, the COMe-cDV7 offers a max of 14x PCIe lanes, 3x USB3.0 ports and 2x SATA ports

Table 8: Intel® Denverton-NS- Atom® Processor Specifications Industrial Temperature

Intel® Denverton Processor	Atom® C3808	Atom® C3708	Atom® C3508	Atom® C3308
# of Cores	12	8	4	2
# of Threads	12	8	4	2
# of HSIO lanes	20 [2]	20 [2]	8 [2]	6 [2]
Processor Base Freq.	2 GHz	1.7 GHz	1.6 GHz	1.6 GHz
Max Turbo Frequency	2 GHZ	1.7 GHz	1.6 GHz	2.10 GHz
TDP	25 W	17 W	11.5	9.5
Cache	12 MB	16 MB	8 MB	4 MB
Memory Types	DDR4-2133	DDR4-2133	DDR4-1866	DDR4-1866
Max.# Mem.Channels	2	2	2	1
Max. MemorySize	256 GB [1]	256 GB[1]	256 GB[1]	128 GB[1]
ECC Memory	Yes	Yes	Yes	Yes
Integrated LAN	4x 10/2.5/1 GbE	4x 10/2.5/1 GbE	4x 2.5/1 GbE	4x 2.5/1 GbE
Intel® Quick Assist (QAT)	Supported			
QAT Speed	High	Medium	Low	Low
QAT Cryptographic Functions	Supported			
QAT Compression / Decompression	Supported			

[1] The COMe-bDV7 supports a max. of 128 GB with 4 SODIMM sockets /respect. 64 GB with 2-SODIMM sockets

[2] The HSIO lanes are shared and used for PCIe, USB3.0, SATA. Depending on the number of supported HSIO lanes, the COMe-cDV7 offers a max of 14x PCIe lanes, 3x USB3.0 ports and 2x SATA ports

Not all items specified in Table 7 and Table 8 are compatible with the COMe-bDV7's functional specification. For more information on specific COMe-bDV7 supported features, see the relevant subheading in this Chapter, and Table 7 and Table 8 foot notes [1] and [2]

3.3. System on a Chip (SoC)

The Intel® Atom® Denverton-NS product family is a SoC solution with integrated Platform Controller Hub (PCH).

The following table lists specific SoC features.

USB	USB 3.0
SATA	SATA Gen.3
LAN	Quad Ethernet ports with up to 10 Gb
VT-d	Supported
PCIe Clock Buffer	3 Clocks supported (GbE, COMe connector, XDP debug connector)

3.4. System Memory

Two DDR4 SODIMM sockets support a maximum of up to 64 GBytes (ECC/non ECC) system memory. As an option, four DDR4 SODIMM can be assembled for a maximum of up to 128 GBytes of (ECC/non ECC) system memory, where the two additional SODIMMs are assembled on the bottom side of the module, see Figure 6: Module Top and Bottom SODIMM Assembly (Option).

The two additional SODIMM sockets on the bottom side of the module increase the height of the on-board components and therefore modules assembled with four SODIMM sockets only fit on a carrier board with an 8 mm high COMe connector. This additional height requirement must be considered when designing the carrier board. For more information, see Chapter 8.2.1: Module Height with Four SODIMM Memory Sockets.

The following table lists specific system memory features.

Socket	2x DDR4 SODIMM (Option: 4x DDR4 SODIMM)
Memory Type	**Default: One SODIMM per channel for up to 32 GB per channel** Channel A: DDR4-2400 SODIMM up to32 GB non-ECC/ECC Channel B: DDR4-2400 SODIMM up to32 GB non-ECC/ECC **(Option: Two SODIMMs per channel for up to 32 GB per channel)** (Channel A: DDR4-2400 SODIMM up to32 GB + 32 GB non-ECC/ECC) (Channel B: DDR4-2400 SODIMM up to32 GB + 32 GB non-ECC/ECC)
Memory Module Size	4 GByte, 8 GByte, 16 GByte and 32 GByte
Peak Bandwidth	34.1 GB/s at 2400 MT/s
Total Height	8 mm with one SODIMM per channel (top side assembly only) 16 mm with two SODIMMS per channel (top and bottom side assembly)

In general, memory modules have a much lower longevity than embedded motherboards, and therefore the EOL of the memory modules may occur several times during the lifetime of the module. Kontron guarantees to maintain memory modules by replacing EOL memory modules with another similar type of qualified module.

As a minimum, it is recommend to use Kontron memory modules for prototype system(s) in order to prove the stability of the system and as a reference.

For volume production, if required, test and qualify other types of RAM. In order to qualify RAM it is recommend to configure three systems running a RAM Stress Test program in a heat chamber at 60°C, for a minimum of 24 hours.

For a list of Kontron memory modules, see Table 6: Memory Modules.

3.5. USB

The COMe-bDV7 standard USB configuration is three USB 3.0 ports and three USB 2.0 ports.

The following table lists supported USB features.

USB 3.0 Ports	3x USB 3.0 (Option for 4 x USB 3.0)
USB 2.0 Ports	4x USB 2.0 (Option for 3x USB 2.0)
USB Over Current Signals	2x

3.5.1. USB 3.0

The default is three USB 3.0 ports with an optional fourth USB 3.0 port if SATA1 is implemented as USB 3.0 port (USB_SS3). All USB 3.0 ports are backwards compatible with the USB 2.0 specification.

The following table lists the COMe connector port and SoC pin combinations for USB 3.0.

COMe Port	SoC HSIO Port [1]	Comments
USB_SS0	16	USB 3.0 port 0
USB_SS1	17	USB 3.0 port 1
USB_SS2	18	USB 3.0 port 2
SATA1/ (USB_SS3)	19	USB 3.0 port 3 (Default is SATA port with an option for USB 3.0 port)

[1]For more details information on the SoC HSIO port usage, see Chapter 3.9: SoC High-speed Interfaces Overview.

3.5.2. USB 2.0

The default is four USB 2.0 ports with an optional for three USB 2.0 ports if Kontron's Security chip solution assembled on USB 2.0 port 3. In total a maximum of eight USB 2.0 ports can be supported when the all the available USB 3.0 ports are implements as USB2.0. For more information regarding Kontron's security chip, see Chapter 9.10: Security Solution (APPROTECT).

The following table lists the COMe connector port and SoC pin combinations for USB 2.0.

COMe Port	USB 2.0 (SoC Pin)	Comments
USB0	USB2_DP/N[0]	USB 2.0 port 0
USB1	USB2_DP/N[1]	USB 2.0 port 1
USB2	USB2_DP/N[2]	USB 2.0 port2
USB3	USB2_DP/N[3]	USB 2.0 port 3 (Default is USB 2.0 port with an option for security chip WIBU assembly)

3.6. SATA

The SATA high-speed storage interface supports two SATA Gen.3 ports with transfer rates of up to 6 Gb/s. SATA1 can be implemented as a USB 3.0 port (USB_SS3).

The following table lists the COMe connector port and SoC port combinations for SATA.

COMe Port	SoC HSIO Port [1]	Comment
SATA0	11	SATA Gen.3, 6 Gb/s
SATA1/ (USB_SS3)	19	SATA Gen.3, 6 Gb/s (Default is SATA port with an option for USB 3.0 port)

[1]For more details information on the SoC HSIO port usage, see Chapter 3.9: SoC High-speed Interfaces Overview.

3.7. PCI Express (PCIE) Configuration

The COMe-bDV7 supports up to 14-HSIO PCIe Gen 3 lanes routed directly to the COMe connector. The number of available PCIe lanes depends on the C3000 processor variant.

The maximum available 14-PCIe lanes are configurable in the BIOS setup with x1, x2, x4 and x8 configuration options. PCIe lanes [6-9], PCIe lanes [8-15] and PCIe lanes [24-31] lanes are not available for use. For the default PCIe configuration options for the supported number of HSIO ports, see Chapter 3.9: SoC High-speed Interfaces Overview.

The following table lists the supported PCIe Gen. 3 port options for COMe lanes.

COMe Lane	SoC HSIO Port	Configuration Options				Comment
		(x1)	(x2)	x4)	(x8)	
PCIE0	12	x1	x2	x4		PCIe lane
PCIE1	13	(x1)				Feature on request: PCIe lane x1 [1]
PCIE2	14	x1	x2			PCIe lane
PCIE3	15	(x1)				Feature on request: PCIe lane x1 [1]
PCIE4	8	x1	x2			PCIe lane
PCIE5	9	(x1)				Feature on request: PCIe lane x1 [1]
PCIE16	0	x1	x2	x4	x8	PCIe lanes
PCIE17	1					
PCIE18	2	x1	x2			
PCIE19	3					
PCIE20	4	x1	x2	x4		
PCIE21	5					
PCIE22	6	x1	x2			
PCIE23	7					

[1] When configuring the PCIe lanes as x1 the 2nd lane of the PCIe pair is not available, however configurations can be offered on request to allow PCIe x1 usage for COMe Lane PCIE0-PCIE5.

3.8. Ethernet

To support network intensive implementations, the COMe-bDV7 features the following Ethernet controllers:

- Quad Ethernet ports with up to 10 Gb (depending on C3000 processor variant)
- 1x 1 Gb Ethernet

3.8.1. Quad Ethernet Ports with up to 10Gb

The Intel® Atom® Processor C3000 series features two integrated Ethernet controllers with two ports each with the following configurations depending on the C3000 processor variant:

- 2x 10 GbE + 2x 10 GbE
- 2x 10 GbE + 2x 2.5GbE
- 2x 2.5 GbE + 2x 2.5 GbE

The two integrated Ethernet controllers support the following operation modes with the corresponding configuration of the LAN-SPI-flash:

Backplane:

- 10GBASE-KR (speed: 10Gb) – default configuration. for 10G ports
- 1000BASE-KX (speed: 1Gb)
- 2500BASE-X (speed: 2.5 Gb) is not an IEEE standard, supports 2.5 G data rate only – default configuration. for 2.5G ports

SFP+:

- SFI (speed: 10Gb) - only supported by 10G ports, native SFI – no additional PHY on the carrier board required
- KR (speed 10Gb)- only supported by 10G ports , requires an external PHY (Inphi) on the carrier board

10GBASE-T:

- KR (speed: 10Gb) – only supported by 10G ports , requires an external PHY (Intel) on the carrier board

1000BASE-T:

- SGMII (speed: 1Gb) – requires an external PHY (Marvell) on the carrier board
- KX (speed: 1Gb) – only supported by 10G ports , requires an external PHY (Intel) on the carrier board

The following table lists the Ethernet Controller's network features.

Data Rate	10 Gb/s 10GBASE-KR (IEEE802.3 KR specification) 1 Gb/s 1000BASE-KX (IEEE802.3 KX specification)
Full Duplex Operation	At all supported speeds
MDIO Interface	Clause 45
Jumbo Frames	Up to 15.5 KB in basic mode 9.5 KB if virtualization or OS2BMC is enabled
VLAN Support	802.1q VLAN Double VLAN
Flow Control Support	Send/receive pause frames and receive FIFO thresholds
Statistics for Management and RMON	Supported
IEEE 1588	Supported

3.8.2. On-board Gigabit Ethernet (1GbE)

An on-board Gigabit Intel® I210IT Ethernet controller connects the SoC high-speed I/O port [10] to the carrier board Management Controller (BMC) and acts as a single port Ethernet controller, in both commercial and industrial temperature environments.

Additionally, the Intel® I210IT Ethernet controller manages the use of:

- NC-SI
- SMBus
- MCTP over PCIE/SMBUS to enable reporting and control of information exposed to LOM device via the NC-SI

The following table lists supported Intel® i210IT Ethernet controller features.

Port Configuration	Single
Data Rate per Port	1 GbE
Interface Type	PCIe v2.1 (2.5 GT/s)
NC-Sideband Interface	Supported
Jumbo Frames	Supported
Interfaces Supported	1000Base-T
IEEE 1588	Supported

3.9. SoC High-speed Interfaces Overview

The following table shows the SoC high-speed serial interface ports utilization and the default COMe PCIe configurations for each HSIO port combination are:

Ports		SoC HSIO Utilization								Description
SoC HSIO	COMe	6-Ports		8-Ports		12-Ports		20-Ports[1]		
		COMe default	PCIe default config.	COMe default	PCIe default config.	COMe default	PCIe default config.	COMe default	PCIe default config.	
19	SATA1/ USB_SS3	SATA1		SATA1		SATA1		SATA1		SATA Gen. 3 or USB 3.0
18	USB_SS2							USB_SS2		USB 3.0
17	USB_SS1					USB_SS1		USB_SS1		
16	USB_SS0			USB_SS0		USB_SS0		USB_SS0		
15	PCIE3					PCIE3	x4	PCIE3	x4	PCIe lane
14	PCIE2					PCIE2		PCIE2		
13	PCIE1			PCIE1	x2	PCIE1		PCIE1		
12	PCIE0	PCIE0	x1	PCIE0		PCIE0		PCIE0		
11	SATA0	SATA0		SATA0		SATA0		SATA0		SATA Gen. 3
10	GBE	GBE		GBE		GBE		GBE		1 GbE Port
9	PCIE5					PCIE5	x2	PCIE5	x2	PCIe lane
8	PCIE4	PCIE4	x1	PCIE4	x1	PCIE4		PCIE4		
7	PCIE23							PCIE23	x8	
6	PCIE22							PCIE22		
5	PCIE21							PCIE21		
4	PCIE20							PCIE20		
3	PCIE19							PCIE19		
2	PCIE18							PCIE18		
1	PCIE17							PCIE17		
0	PCIE16	PCIE16	x1	PCIE16	x1	PCIE16	x1	PCIE16		

[1] SATA 0 is on SATA Controller 0, SATA 1 independently on SATA Controller 1 for higher performance

Different HSIO depends on the SoC. For configuration of the HSIOs (6-ports, 8-ports, 12-ports and 20-ports), the following BIOS setting must be set to disabled: Advanced>Firmware Update Configuration>Disabled.

3.10. Storage

The following table lists the supported storage features.

eMMC	eMMC 5.0 NAND Flash Up to 64 GB pSLC (or up to 128 GB MLC)
SATA AHCI	NCQ, HotPlug, eSATA and Staggered Spinup

Pseudo SLC (pSLC) is reconfigured MLC. pSLC memory capacity is half of the MLC capacity.

3.11. BIOS/Software

The following table lists the supported BIOS and software features.

BIOS EFI	AMI Aptio V UEFI
Software	KeAPI 3.0 for all supported OS EFI Utilities to log and process module information (DMCM tools) BIOS/EFI Flash utility for EFI Shell, Windows, Linux BIOS/EFI utility for customers to implement Boot Logo
Operating System (OS)	Windows® Server 2012/2016 Linux Yocto 64- bit VxWorks 7.x

3.12. COMe Features

The following table lists the supported COM Express® features.

SPI	Boot from an external SPI
LPC	Supported
UART	2x UART (RX/TX)
LID Signal	Supported
Sleep Signal	Supported
SMBus	Speed configurable, default 100 k SMB
RTC	System time and date

3.13. Kontron Features

The following table lists the supported Kontron specific product features.

External I2C Bus	Fast I2C, Multimaster capable
Embedded API	KeAPI 3.0
Customer BIOS Settings / Flash Backup	Supported
Watchdog Support	Dual staged
External SIO	Supported on the carrier board
GPIO	GPI[0:3] and GPO[0:3]
Rapid Shutdown	Supported on E2 variants
Kontron Security Chip (WIBU)	Supported on USB 2.0 port 3 (This option reduces the number of available USB 2.0 ports to 3x USB 2.0)

4/ Electrical Specification

4.1. Power Supply Specifications

Power is supplied by either an ATX (12 V + 5 V standby) or a single power wide range (8.5 V to 20 V).power supply.

The following table lists the power supply specifications.

Supply Voltage (VCC)	12 V
Standby Voltage	5 V ±5%
Supply Voltage Range (VCC)	8.5 V to 20 V (wide range voltage input across the whole temperature range)

4.2. Power Supply Voltage Rise Time

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

4.3. Power Supply Voltage Ripple

The maximum power supply voltage ripple is 200 mV peak-to-peak at 0 MHz – 20 MHz.

4.4. Inrush Current

The maximum inrush current at 5 V standby is 2 A, and from state G3 (Module is mechanically completely off, with no power consumption) or state S5 (module appears to be completely off) to state S0 (module is fully usable) the maximum inrush current meets the SFX Design Guide.

4.5. Power Management

If the supply voltage (VCC) is removed, by applying 5 V ±5% to the COMe connector's 5 V Standby power pins (V_5V_STBY) the following ACPI suspend power states can be supported to save power:

- S4- Hibernate where the module appears to be off and power consumption is kept to a minimum
- S5 – Soft-off states where the modules appears to be off

If the supply voltage is applied to the COMe connector's VCC pins (VCC_12V), the following ACPI wake up power state is supported:

- S0 – Wake-up state where the module is fully functional and supply voltage(VCC) is required to power the module

Power management options for the module and CPU are available within the BIOS setup:

- Advanced>ACPI Settings>>Enable ACPI Auto Config>Enable/Disable
- Advanced>Lid Switch Mode>Enable/Disable
- Advanced>Sleep Button Mode>Enable/Disable
- IntelRCSetup>Processor Configuration>ACPI 3.0 T-states>Enable/Disable

For further ACPI information, see Chapter 9.1: ACPI Power States.

4.6. Power Supply Control Settings

The power supply control settings are set in the BIOS and enable the module to shut down, rest and wake from standby properly.

The following table lists the implemented power supply control settings.

Power Button (PWRBTN#)	Pin B12	To start the module using the power button, the PWRBTN# signal must be at least 50 ms (50 ms ≤ t < 4 s, typical 400 ms) at low level (Power Button Event). Pressing the power button for at least four seconds turns off power to the module (Power Button Override).
Power Good (PWR_OK)	Pin B24	PWR_OK is internally pulled up to 3.3 V and must be at the high level to power on the module. This can be driven low to hold the module from powering up as long as needed. The carrier needs to release the signal when ready. Low level prevents the module from entering the S0 state (Wake up event). A falling edge during S0 (Wake up event) causes a direct switch to S5 (Power Failure).
Reset Button (SYS_RESET#)	Pin B49	When the SYS_RESET# pin is detected active (falling edge triggered), it allows the processor to perform a "graceful" reset, by waiting up to 25 ms for the SMBus to go idle before forcing a reset, even though activity is still occurring. Once the reset is asserted, it remains asserted for 5 ms to 6 ms regardless of whether the SYS_RESET# input remains asserted or not.
SM-Bus Alert (SMB_ALERT#)	Pin B15	With an external battery manager present and SMB_ALERT #connected, the module always powers on even if the BIOS switch "After Power Fail" is set to "Stay Off".
Battery low (BATLOW#)	Pin A27	BATLOW# can be used as a power fail indication a Type 7 system where assertion prevents wake from S3-S5 states.

4.7. Power Supply Modes

Setting the power supply controls enables the COMe-bDV7 to operating in either ATX power mode or in single power supply mode.

4.7.1.1. ATX Modes

To start the module in ATX mode and power VCC, follow the step below.

1. Connect the ATX PSU with VCC and 5 VSB, to set PWR_OK to low and VCC to 0 V.
2. Press the power button to set the PWR_OK to high and power VCC.

The PS_ON# signal generated by SUS_S3# (A15) indicates that the system is in the Suspend to RAM state. An inverted copy of SUS_S3# on the carrier board may be used to enable non-standby power on a typical ATX supply. The input voltage must always be higher than 5 V standby (VCC > 5 VSB) for Computer-On-Modules supporting a wide input voltage range down to 8.5 V.

The following table lists the ATX mode settings.

State	PWRBTN#	PWR_OK	V5_StdBy	PS_ON#	VCC
G3	X[1]	x	0 V	x	0 V
S5	high	low	5 V	high	0 V
S5 → S0	PWRBTN Event	low → high	5 V	high→ low	0 V→ VCC
S0	high	high	5 V	low	VCC

[1]Signals are not relevant for the specific power state. It makes no difference if the signal is connected or open.

4.7.1.2. Single Supply Mode

In single supply mode, without 5 V standby, the module starts automatically if VCC power is connected and the Power Good input is open or at the high level (internal PU to 3.3 V).

PS_ON# is not used in single supply mode and the input voltage VCC range can be 8.5 V to 20 V.

To power on the module from S5 state, press the power button or reconnect VCC. Suspend/Standby states are not supported in single supply mode.

The following table lists the single supply mode settings.

State	PWRBTN#	PWR_OK	V5_StdBy	VCC
G3	x[1] / 0 V	x [1]/ 0 V	x[1] / 0 V	0 V
G3 → S0	high	open / high	open	connecting VCC
S5	high	open / high	open	VCC
S5 → S0	PWRBTN Event	open / high	open	reconnecting VCC

[1] Signals are not relevant for the specific power state. It makes no difference if the signal is connected or open.

All ground pins must be connected to the carrier board's ground plane.

5/ Thermal Management

5.1. Heatspreader and Active or Passive Cooling Solutions

A heatspreader plate assembly is available from Kontron for the COMe-bDV7. The heatspreader plate assembly is NOT a heat sink. The heatspreader works as a COM Express® standard thermal interface to be use with a heat sink or external cooling devices.

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

- 60°C for commercial temperature grade modules
- 85°C for industrial temperature grade modules (E2)

5.2. Active or Passive Cooling Solutions

Both active and passive thermal management approaches can be used with heatspreader plates. The optimum cooling solution varies, depending on the COM Express® application and environmental conditions. Active or passive cooling solutions provided from Kontron for the COMe-bDV7 are usually designed to cover the power and thermal dissipation for a commercial temperature range used in housing with proper airflow.

For more information concerning possible cooling solutions, see Chapter 2.5 Accessories.

5.3. Operating with Kontron Heatspreader Plate (HSP) Assembly

The operating temperature defines two requirements:

- Maximum ambient temperature with ambient being the air surrounding the module
- Maximum measurable temperature on any part of the heatspreader's surface

The heatspreader is tested for the temperature specifications listed in the table below.

Table 9: Heatspreader Test Temperature Specifications

Temperature Specification	Validation Requirements
Commercial Grade	at 60°C HSP temperature the CPU @ 100% load needs to run at nominal frequency
Industrial Grade by screening (E2)	at 85°C HSP temperature the CPU @ 50% load is allowed to start throttling for thermal protection

HOT Surface!
Do NOT touch! Allow to cool before touching.

5.4. Operating without Kontron Heatspreader Plate (HSP) Assembly

The operating temperature is the maximum measurable temperature on **any** part of the module's surface.

5.5. On-board Fan Connector

The module's 3-pin fan connector powers, controls and monitors a fan for chassis ventilation.

Figure 3: Fan Connector 3-Pin

Table 10: Fan Connector (3-Pin) Pin Assignment

Pin	Signal	Description	Type
1	Fan_Tach_IN#	Input voltage	I
2	V_FAN	Limited to a max. 12 V (±10%) across the whole input range	PWR
3	GND	Power GND	PWR

To connect a standard 3-pin connector fan to the module, use one of the following adaptor cables:

- KAB-HSP 200 mm (Part number - 96079-0000-00-0)
- KAB-HSP 40 mm (Part number - 96079-0000-00-2)

NOTICE

Always check the fan specification according to the limitations of the supply current and supply voltage.

If the input voltage is below 13 V, the maximum supply current to the on-board fan connector is 350 mA. The maximum supply current is further limited to 150 mA if the input voltage is between 13 V and 20 V. For an overview of the electrical characteristics, refer to Table 11.

Table 11: Electrical Characteristics of the Fan Connector

Module Input Voltage	FAN Output Voltage	FAN Output Current
< 13 V	8.5 V to 13 V	350 mA Max.
13 V to 20 V	12 V (± 10%)	150 mA

6/ Environmental Specification

6.1. Temperature

Kontron defines the following temperature grades for Computer-On-Modules. For more information on the available temperature grades for the COMe-bDV7, see Chapter 2.1: Module Variants.

Table 12: Temperature Grade Specifications

Temperature Grades	Operating	Non-operating / Storage
Commercial Grade	0°C to +60°C	-30°C to +85°C
Industrial Grade E2	-40°C to +85°C	-40°C to +85°C

6.2. Humidity

Table 13: Humidity Specification

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

7/ Standards and Certification

The COMe-bDV7 complies with the listed European Council directives or the latest status thereof:

- European Council directive relating to Electromagnetic Compatibility (2014/30/EU)
- General Product safety Directive (2001/95/EC)
- Low Voltage directive (2014/35/EU)

Table 14: Standards and Certification Compliance, provides information regarding standards that are elements of the CE declaration and additional standard compliancy information. For more information, contact Kontron Support.

Table 14: Standards and Certification Compliance

EMC	**Emission**	EN 55032 (CISPR 32) Electromagnetic compatibility of multimedia equipment- emission requirements IEC/ EN 61000-3-2: Limits for harmonic current emissions IEC/ EN 61000-3-3: Limits for Voltage changes, voltage fluctuations and flicker
	Immunity	EN 55024 (CISPR 24) Information Technology Equipment- Immunity characteristics- Limits and methods of measurements EN 61000-6-2 Generic Standards immunity for industrial environments + CENELEC – Cor
Safety/CE		EN/IEC 62368-1 Safety requirements for audio/video, information, and communication technology equipment UL 60950-1/CSA 60950-1 (component recognition) Information Technology Equipment Including Electrical Business Equipment NWGQ2.E304278 NWGQ8.E304278
Shock		IEC/EN 60068-2-27 Non-operating shock – (half-sinusoidal, 11 ms, 15 g)
Vibration		IEC/EN 60068-2-6 Non-operating vibration – (sinusoidal, 10 Hz – 2000 Hz, +/- 0.15 mm, 2 g)
Theoretical MTBF		System MTBF (hour) = 560342h @ 40°C for COMe-bDV7 C3958 (Reliability report article number: 68006-0000-58-9) System MTBF (hour) = 533426h @ 40°C for COMe-bDV7 R E2 C3808 (Reliability Report article number: 68007-0000-08-8)
RoHS		directive 2011/65/EU Restriction of Hazardous substance in electrical and Electronic Equipment (RoHS)
WEEE		Directive 2012/19/EU Waste Electrical and Electronic Equipment (WEEE)
REACH		Regulation (EC) No. 1907/2006 Registration, Evaluation, Authorization and Restriction of Chemicals (REACH)

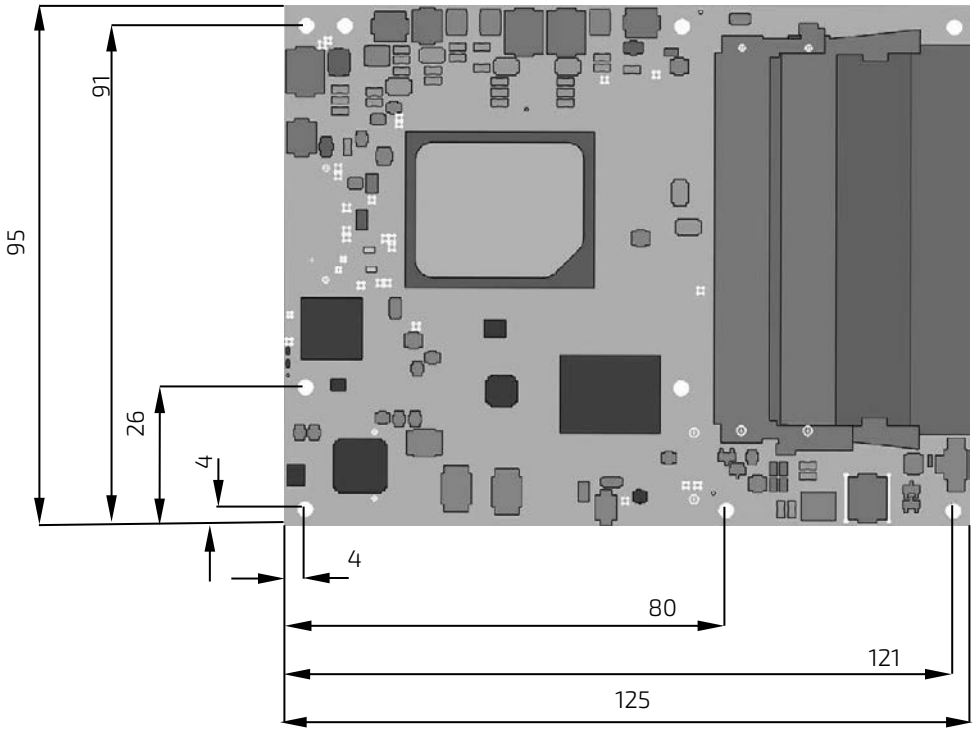
8/ Mechanical Specification

The mechanical specification of the standard COMe-bDV7 basis COM Express® PICMG COM.0 Rev 3.0 Type 7 module.

8.1. Dimensions

The overall dimensions of the basic module are 125 mm x 95 mm.

Figure 4: Module Dimensions

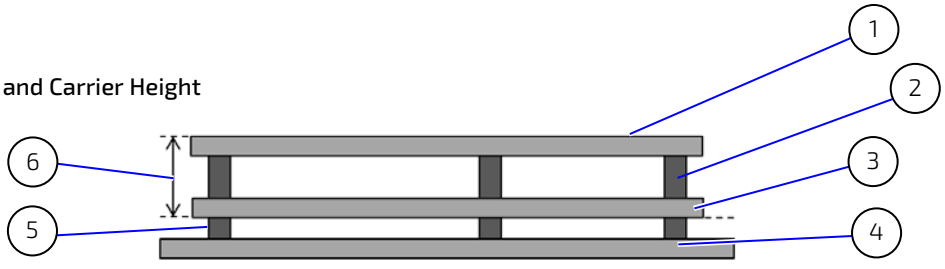


*All dimensions in mm.

CAD drawings are available at EMD Customer Section.

8.2. Height

Figure 5: Module and Carrier Height



1	Heatspreader	4	Carrier PCB Board
2	Heatspreader standoff(s)	5	Connector standoff(s) 5 mm or 8 mm
3	Module PCB board	6	13 mm +/- 0.65 mm

The COM Express® specification defines a module height of approximately 13 mm from the bottom of the module's PCB board to the top of the heatspreader, as shown in Figure 3: Module and Carrier Height. The overall height of the module and carrier board depends on maximum memory requirement and the implemented cooling solution.

8.2.1. Module Height with Four SODIMM Memory Sockets

The overall height of the module and carrier board depends on whether the COMe-bDV7 is implemented with:

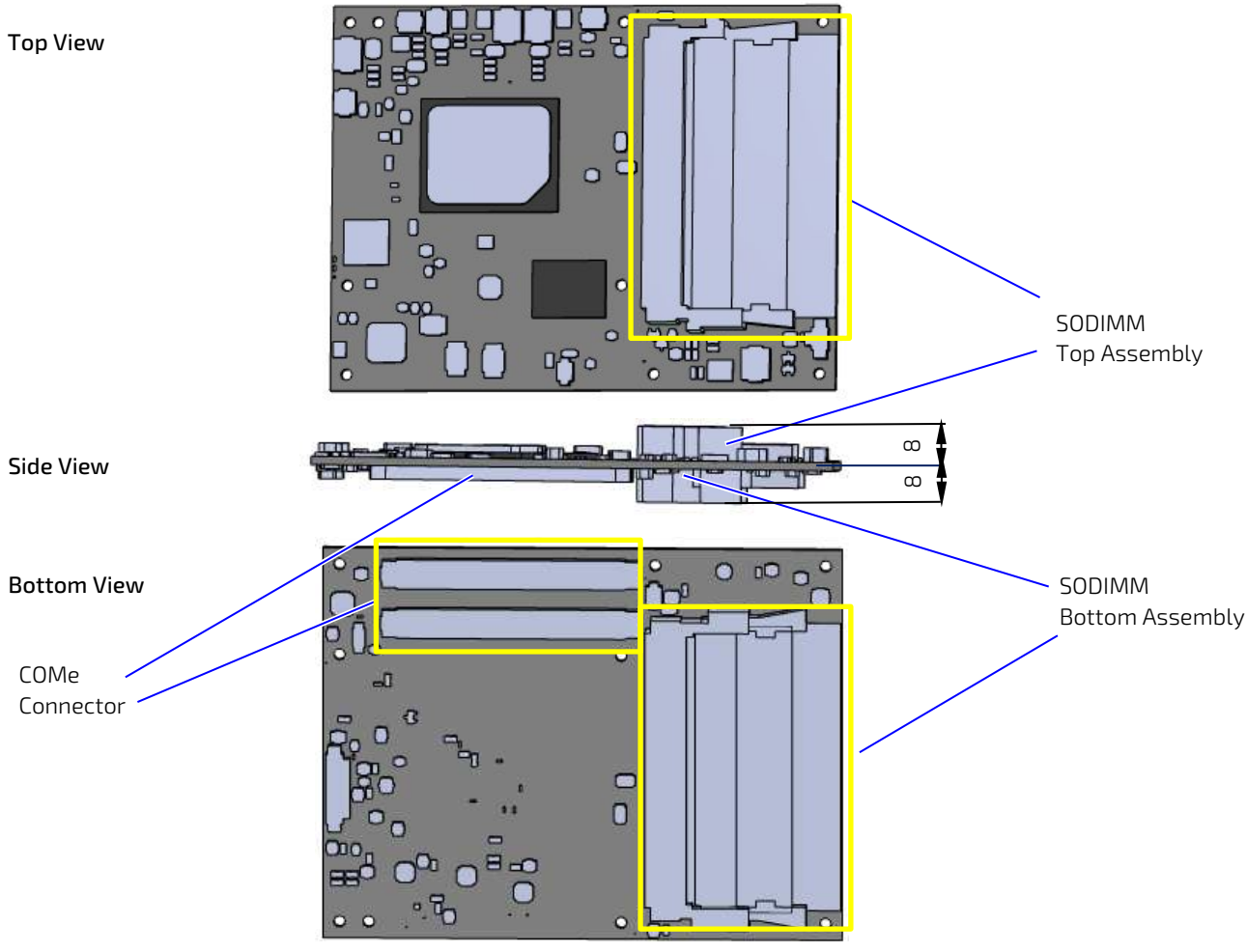
- two SODIMMs both located on module's top side (standard variant)
- four SODIMMs with two located on module's top side and bottom side

The COMe-bDV7 variant with four SODIMM memory is outside the basis COM Express® PICMG COM.0 Rev 3.0 Type 7 module form factor and requires the carrier board to be designed to support an 8 mm high COMe connector, see Table 6. To calculate the total height of the module and carrier take both the top side height and the bottom side height into consideration.

The 4x SODIMM variant has SODIMM sockets assembled on the bottom side of the module and requires a carrier board with 8 mm high COMe connectors and a component free area on the carrier board below the module SODIMM sockets.

The following figure shows the module board with the optional variant SODIMMs assemble on the top side and the bottom side of the board.

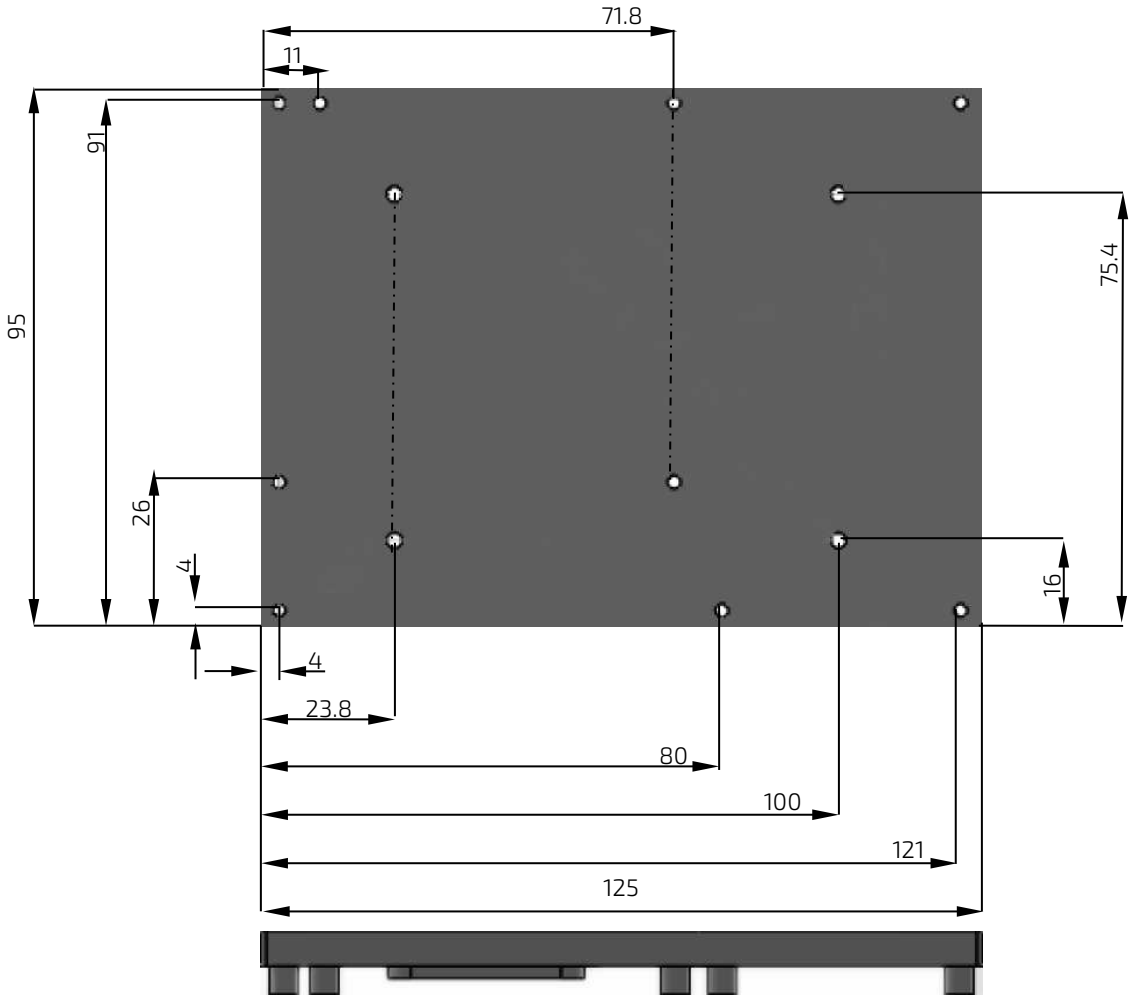
Figure 6: Module Top and Bottom SODIMM Assembly (Option)



8.3. Heatspreader Dimensions

The following figure shows mounting holes for additional cooling solutions.

Figure 7: Heatspreader Dimensions



*All dimensions in mm.

9/ Features and Interfaces

9.1. ACPI Power States

The Advanced Configuration and Power Interface (ACPI) 4.0 enables the system to power down and save power when not required (suspend) and wake up when required (resume). The ACPI controls the power states S0-S5, where S0 has the highest priority and S5 the lowest priority. The COMe-bDV7 comes with ACPI 4.0 and supports the power states S1, S4, S5 only.

Not all ACPI defined states are available.
SoC systems that support the low-power idle state do not use S1-S3.

Table 15: Supported Power States Function

S0	Wake-up-event state
S4	Suspend-to-disk / Hibernate
S5	Soft-off state

The following events resume the system from S4 (Suspend-to-disk / Hibernate):

- Power Button
- WakeOnLan

The following events resume the system from S5 (Soft-off state):

- Power Button
- WakeOnLan

OS must support wake up by USB devices and carrier board must power USB Port with StandBy-Voltage. Depending on the used Ethernet MAC/Phy, WakeOnLan must be enabled in the BIOS Setup and driver options.

9.2. eMMC Flash memory

An optional embedded Multimedia Flash Card (eMMC) complying with the eMMC 5.0 specification can be permanently attached to the module, allowing for a capacity of up to 64 GByte NAND Flash. During the COMe-cAL6's manufacturing process, Multi Level Cell (MLC) eMMC is reconfigured to act as a pseudo Single Level Cell (pSLC) eMMC to provide improved reliability, endurance and performance.

Specific eMMC Flash memory features are:

- Up to 64 GByte pSLC (or up to 128 GByte MLC)
- eMMC 5.0 specification
- Class 0 (basic); class 2 (block read); class 4 (block write); class 5 (erase); class 6 (write protection); class 7 (lock card)
- HS200/HS400 modes
- DDR modes up to 52 MHz clock speed
- ECC and block management
- Boot operation (High-speed boot)
- Sleep mode
- Permanent and power-on write protection
- Replay-protected memory block (RPMB)
- Secure erase and secure trim

9.3. Fast I2C

Fast I2C supports transfer between components on the same board with data transfers up to 400 kHz. The I2C bus uses two bus line and a simple master /slave relationship for signals between components and each component is addressable with a unique software address. For information in the I2C system resources addresses, see Chapter 10.5: I2C Bus. The internal I2C bus speed is selected in the BIOS setup where the I2C bus speed ranges between (1 kHz and 400 kHz). For a default system, 200 kHz is appropriate. For more information on the BIOS set up, refer to Chapter 12/ uEFI BIOS.

The COMe-bDV7 on-board I2C controller connects to the LPC bus (LPC2I2C), and to the on-board EEPROM and COM Express® connector.

The I2C controller supports:

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

9.4. GPIO

Eight GPIO pins are available, with four pins for the in-direction (pin A54 for GPI0, pin A63 for GPI1, pin A67 for GPI2 and pin A85 for GPI3) and four pins for the out-direction (pin A93 for GPO0, pin B54 for GPO1, pin B57 for GPO2 and pin B63 for GPO3). The type of termination resistor on the module sets the direction of the GPIO where GPIs are terminated with pull-up resistors and GPOs are terminated with pull-downs resistors.

Due to, the fact that both the pull-up and pull-down termination resistors are weak, it is possible to override the termination resistors using external pull-ups, pull-downs or IOs. Overriding the termination resistors means that the eight GPIO pins can be considered as bi-directional since there are no restrictions whether you use the available GPIO pins in the in-direction or out-direction.

9.5. HWM

The HardWare Monitor (HWM) controls the health of the system by monitoring critical aspect such as temperatures, power supply voltages and fan speed for cooling. The temperature is controlled by temperature sensors supported via the SMBus interface and directly from the CPU using Intel's® PECI3.0 interface. The SMART FAN ™ technology controls the duty cycle of the fan output with temperature setting points. This enables flexible fan control for cooling solutions and noise sensitive solutions. For system protection, users can set threshold values for alarm signals.

9.6. Hyper Threading

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

9.7. LPC

The Low Pin Count (LPC) Interface signals are connected to the LPC Bus bridge located in the Soc. 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 subsystem complies with the COM Express® specification. The COM Express® Design Guide maintained by PICMG provides implementation information or refer to the official PICMG documentation for more information.

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. This leads to limitations for ISA bus and SIO (standard I/O(s) like floppy or LPT interfaces) implementation. The COMe-bDV7 LPC clock buffer allows for the connection of three LPC devices

All Kontron COM Express® Computer-on-Modules include BIOS support for the following external carrier board LPC Super I/O controller features for the HWM chip Nuvoton NCT7802Y.

Table 16: Supported BIOS Features

HWM Feature	AMI EFI APTIO V
COM1/COM2, FPGA, TPM	Supported
PS/2, LPT, HWM, Floppy, GPIO	Not supported

Features marked as not supported do not exclude OS support, except for, HWM that is controlled within the BIOS Advanced setup menu and has no OS software support. The HWM is accessible via the System Management (SM) Bus. For more information, see Chapter 10.6: System Management (SMBus)

If any other LPC Super I/O additional BIOS implementations are necessary, contact Kontron Support.

9.8. Radid Shutdown

Kontron has implemented a rapid shutdown function on R E2 modules variants. Rapid shutdown performs a controlled accelerated system shutdown and functions as follows:

1. An active-high shutdown signal is asserted by the COM Express Eval Type 7 carrier board through pin C67 of the COM Express connector. The characteristics of the shutdown signal are as follows:

   - Amplitude 5.0 V +/- 5%
   - Source impedance < = 50 ohms
   - Rise time ⇐ 1 µs
   - Duration >= 20 µs

   The assertion of this signal causes all power regulators to be disabled and the internal power supply rails to be discharged by crowbar circuits. The shutdown circuitry provides internal energy storage that maintains crowbar activation for at least 2 ms following the de-assertion of the shutdown signal. The circuit also incorporates a weak input pull-down resistor so that the module operates normally in systems where the rapid shutdown functionality is not used and pin C67 (RAPID_SHUTDOWN) of the COMe connector is left unconnected.

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

3. Simultaneously with the leading edge of shutdown, the 5 V (standby) input power to the module is removed, if present. External clamping on these pins is not necessary (but recommended) because it is clamped through the module by the main 12 V rail.

9.8.1. Crowbar

Crowbar circuits are designed to meet the following criteria on each rail, when the shutdown signal is asserted:

- Voltage decays to 37% of initial value (equivalent to one RC time constant) within 400 µs
- Voltage decreases to below 1.5 V within 2 ms

It is customary that the design of carrier's crowbar on the 12 V and 5 V rails is based on similar criteria.

9.9. Quick Assist Technology (Intel® QAT)

The Intel® Quick Assist Technolg0 (QAT) improves the performance of systems used in applications such as the cloud, networking, big data and storage by speeding up cryptographic workloads. Intel® QAT achieved this by offloading data to hardware capable of optimizing cryptology functions such as integrated built-in cryptographic accelerators and security applications.

This gives users the flexibility to choose different cryptographic accelerators and to scale using multiple cryptographic accelerators if required.

To use the Intel® Quick Assist Technology® refer to the operating systems compatibility information.

9.10. RTC

The Real Time Clock (RTC) keeps track of the current time accurately. The RTC's low power consumption means that the RTC can be powered from an alternate source of power enabling the RTC to continue to keep time while the primary source of power is off or unavailable.

A typical RTC voltage is 3 V with a current of less than 10 µA if the module is powered by the mains supply the RTC voltage is generated by on-module regulators to reduce RTC current draw.

9.11. Security Solution (APPROTECT)

Kontron's Security Solution is a security chip for Kontron's security stack (APPROTECT). This combined hardware and software solution is an embedded hardware security chip with software framework to provide full protection for your application. The integrated security chip connected to USB2 port 3, supports the following features:

- Copy protection
- IP protection
- License model enforcement

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

9.12. SMBus

System Management Bus (SMBus) is a 2-wire serial interface used to connect several devices. The SMBus's low bandwidth makes the SMBus ideal for power related signals with low data content. The SMBus supports fan sensors, temperature sensors and voltage sensors.

9.13. SpeedStep® Technology

SpeedStep® technology enables you to adapt high performance computing to your applications by switching automatically between maximum performance mode and battery-optimized mode, depending on the needs of the application. When battery powered or 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 high frequency, allowing you to customize performance.

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

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

9.14. Serial peripheral Interface (SPI)

The Serial Peripheral Interface Bus (SPI bus) is a synchronous serial data link standard. Devices communicate in master/slave mode, where the master device initiates the data frame. Multiple slave devices are allowed with individual slave select (chip select) lines. SPI is sometimes called a four-wire serial bus, contrasting with three, two and one-wire serial buses.

The COMe-bDV7 module contains two SPI chips (primary SPI flash and secondary SPI flash) and can use an external SPI chip on the carrier board for booting.

9.14.1. SPI boot

The COMe-bDV7 supports boot from a 16 MB 3V serial external SPI Flash. To configure the SPI Flash to be used for booting, placing jumpers on pin A34 (BIOS_DIS0#) and pin B88 (BIOS_DIS1#) as follows:

Table 17: SPI Boot Configuration

Configuration	BIOS_DIS0#	BIOS_DIS1#	Function
1	Open	Open	Module SPI only
2	GND	Open	Not supported
3	Open	GND	Carrier board SPI Only
4	GND	GND	Not supported

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

If the Firmware Update Configuration is set to Enabled (Advanced>Firmware Update Configuration>Enabled), it is possible to flash in the BIOS setup and override the platform configuration on FIA/WM to make changes within the BIOS. These changes will be implemented in the next cycle. Once the changes have been made the BIOS setting will automatically be reset to disabled (Advanced>Firmware Update Configuration>Disabled).

Each time changes are to be made within the BIOS setup, the Firmware Update Configuration must be set to enabled (Advanced>Firmware Update Configuration>Enabled). It is not possible to set the Firmware Update Configuration permanently to enabled, as this prevents HSIO lane configuration. For more information, see 3.9: SoC High-speed Interfaces Overview.

After flashing the BIOS set up the Firmware Update Configuration is set to disabled on the next cycle. For further changes Firmware Update Configuration must be reset to enabled.
NOTE: It is not possible to set the Firmware Update Configuration permanently to enabled, as this prevents HSIO lane configuration.

To Flash to an SPI chip that is not the boot SPI Flash chip, see Chapter 9.13.3: Using an External SPI Flash.

Table 18: Supported SPI Boot Flash Types for 8-SOIC Package

Size	Manufacturer	Part Number	Device ID
128 Mb (16 M x8)	Micron Technology	MT25QL128ABA1ESE-0SIT	0xBA18
128 Mb (16 M x8)	ISSI	IS25LP128-JBLE	0x4018
128 Mb (16 M x8)	Winbond	W25Q128JVSIQ	0x6018

9.14.2. Module SPI Flash Chips

The module contains two SPI chips (primary SPI flash and secondary SPI flash). Both the primary and secondary SPI flash chips contain a factory installed BIOS version. If the primary SPI flash is configured with a non-working BIOS and it is not possible to boot from the primary SPI flash, after a set period of time the system switches to the secondary SPI flash and performs a reset and automatically boots from the secondary SPI flash. After booting, the communication must is then switched back to the primary SPI flash to avoid re-flashing the secondary SPI flash.

9.14.3. Using an External SPI Flash

Initially, boot on the EFI Shell with an USB key containing the binary used to flash the SPI, plugged in on the system. Depending on which SPI you would like to flash, you will need to use the (BIOS_DIS1#) jumper located on the COM Express® carrier.

To flash the carrier or module Flash chip:

1. Connect a SPI flash with the correct size (similar to BIOS binary (*.BIN) file size) to the carrier SPI interface.
2. Open pin A34 (BIOS_DIS0#) and pin B88 (BIOS_DIS1#) to boot from the module BIOS.
3. Turn on the system and make sure your USB is connected, then start the setup.
4. The BIOS Lock is controlled within the “Relax Security Config” BIOS setup. To disable the BIOS lock set:

   InterlRCSetup >Relax Security Config >Enabled

   Enable the local Firmware update by setting:

   Advanced>Firmware Update Configuration>Local FW update>Enabled
5. Save and exit the setup.
6. Reboot system into EFI shell.
7. Connect pin B88 (BIOS_DIS1#) to ground to enable the external SPI flash.
8. From the EFI shell, enter the name of the partition of your USB Key in this example; select FS0: then <enter>.
9. Enter the following:

```
spsFPT.efi –F <biosname.bin>
```

To update to a newer BIOS version, it is recommended to use AMI Flash Utilities (AFU). For more information, refer to the AMI Flash Utilities user guide for options.
The usual command line for AfuEfix64.efi is: `Afuefix64.efi <BIOS Filename> /P /B /N`
To update the local ME Firmware, also add the option "/ME" to the command line.
It is also possible to flash 10G region only by specifying the option "/GBEA" and "/GBEB".

10. Wait until the program ends properly and then power cycle the whole system.
11. The system is now updated.

Depending on the state of the external SPI flash, the program may display up to two warning messages printed in red. Do not stop the process at this point! After a few seconds of timeout, flashing proceeds. For more information, refer to the EMD Customer Section.

9.14.4. External SPI flash on Modules with Intel® ME

If booting from the external (carrier board mounted) SPI flash then exchanging the COM Express® module for another module of the same type will cause the Intel® Management Engine (ME) to fail during the next start. This is due to the design of the ME that bounds itself to every module the ME was flashed to previously. In the case of an external SPI flash, this is the module present at flash time.

To avoid this issue, conduct a complete flash of the external SPI flash device after changing the COM Express® module for another module. If disconnecting and reconnecting the same module again, this step is not necessary.

9.15. TPM 2.0

A 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 chip and cannot be accessed by software. The Storage Root Key (SRK) is created when a user or administrator takes ownership of the system. The TPM generates the key pair 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 that 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.

9.16. UART

The UART implements an interface for serial communications and supports up to two serial RX/TX ports on pin A98 (SER0_TX) and pin A99 (SER0_RX) for UART0, and pin A101 (SER1_TX) and pin A102 (SER1_RX) for UART1.

The UART controller is fully 16550A compatible and supports:

- On-Chip bit rate (baud rate) generator
- No handshake lines
- Interrupt function to the host
- FIFO buffer for incoming and outgoing data

9.17. Virtualization Technology (Intel ® VT)

Intel® Virtualization Technology (Intel® VT) is a portfolio of technologies that enables one hardware platform to function as multiple "virtual" platforms, therefore reducing overhead, improving manageability by limiting downtime, improving productivity by partitioning separate computer activities and improved security in virtual environments.

- Intel® Virtualization Technology (VT-x) – enables multiple "virtual" platforms.
- Intel® Virtualization Technology for Directed I/O (VT-d) - enables I/O-device virtualization
- Intel® VT-x with Extended Page Tables (EPT)- improves memory intensive virtualized applications with hardware optimization of page table management, (also known as Second Level Address Translation (SLAT)

9.18. Watchdog Timer – 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 dual stage watchdog timer works with two stages that can be programmed independently and used stage by stage.

Table 19: Dual Stage Watchdog Timer- Time-out Events

0000b	No action	The stage is off and will be skipped.
0001b	Reset	A reset restarts the module and starts a new POST and operating system.
0010b	NMI	A non-maskable interrupt (NMI) is a computer processor interrupt that cannot be ignored by standard interrupt masking techniques in the system.NMI is used typically to signal attention for non-recoverable hardware errors.
0011b	SMI	A system management interrupt (SMI) makes the processor entering the system management mode (SMM). As such, specific BIOS code handles the interrupt. The current BIOS handler for the watchdog SMI currently does nothing. For special requirements, contact Kontron Support.
0100b	SCI	A system control interrupt (SCI) is a OS visible interrupt to be handled by the OS using AML code.
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 triggers the WDT pin on the carrier board connector (COM Express® pin B27) only

9.18.1. WDT Signal

Watchdog time-out event (pin B27) on the COM Express® connector supports a signal that can be asserted when a watchdog timer has not been triggered within a set time. The WDT signal is configurable to either of the two stages. After reset, the signal is automatically deasserted. If deassertion is necessary during runtime, contact Kontron Support for further help.

9.19. XDP (Option)

The eXtended Debug Port (XDP) enables hardware debugging to be performed on the system using a 60-pin connector. The XDP interface includes a probe adjacent to the XDP connector and connected to the XDP connector via a ribbon cable. A remote system accesses the hardware probe to debug the system.

10/ System Resources

The system resource information is currently in work and not available in this revision of the user guide.

10.1. Legacy Interrupt Request (IRQ) Lines

The following table specifies the device connected to each Interrupt line or if the line is available for new devices.

Table 20: Legacy IRQ Lines

IRQ	General Usage	Project Usage
1	Timer	Timer
2	Keyboard	Keyboard (SuperIO)
3	Redirected secondary PIC	Redirected secondary PIC
4	PCI devices	Free for PCI devices
5	PCI devices	Free for PCI devices
6	LPT2/PCI devices	One of COM3+4
7	FDD	One of COM3+4 or not used
8	LPT1	LPT1 or one of COM3+4
9	RTC	RTC
10	SCI / PCI devices	Free for PCI devices
11	COM2[1]	COM2[1]
12	COM1[1]	COM1[1]
13	PS/2 mouse	PS/2 mouse (or free for PCI devices)
14	FPU	FPU
15	IDE0	Not used

[1] COM1 and COM2 IRQ are valid only for Windows OS. For Linux non-legacy IRQs are used, IRQ16(COM1) and IRQ17(COM2). Configuration is done via „Advanced -> OS Selection“ BIOS option

10.2. Memory Area

The first 640 kB of DRAM are used as main memory (0000-0000 0009-FFFF). Using DOS, you can address the 1 MB of memory directly using special drivers such as HIMEM.SYS and EMM386.EXE, which are part of the operating system. Refer to the operating system documentation or special textbooks for information about HIMEM.SYS and EMM386.EXE. Other operating systems (Linux or Windows versions) allow you to address the full memory area directly

The following table specifies the usage of the address ranges within the memory area.

Table 21: Designated Memory Locations

Address Range (hex)		Size	Project Usage
DOS DRAM 0 to 1 MB			
0000-0000	0009-FFFF	640 KB	DOS (memory)
000A-0000	000B-FFFF	128 KB	VGA (A Segment and B Segment
000C-0000	000D-FFFF	128 KB	DRAM (C Segment and D Segment)
000E-0000	000E-FFFF	64KB	Extended System BIOS [1]
000F-0000	000F-FFFF	64 KB	System BIOS upper F segment[1]
Lower Dram - 1MB to TOLUD (Top of Lower Usage DRAM)			
00F0_0000	0100-0000	1MB	System memory (Low DRAM). This range is always mapped the DRAM .

Address Range (hex)		Size	Project Usage
Lower MMIO TOLUD (Top of Lower Usage DRAM) to 4 GB			
FEB0-0000	FEBF-FFFF		Abort
FEC0-0000	FEC0-0040		I/O(X)APIC
FED0-0000	FED0-03FF		High performance event timer
FED4-0000	FED4-0FFF		TPM- TPM1.2 range
FED6-0000	FED6-0FFF		XHCI DbC - no other MMIO must overlap this address range
FEE0-0000	FEEF-FFFF		Local APIC
FF00-0000 FF10-0000 FF20-0000 FF30-0000	FF0F-FFFF FF1F-FFFF FF2F-FFFF FF3F-FFFF		BIOS4 Feature space for LPC
FF40-0000 FF50-0000 FF60-0000 FF70-0000	FF4F-FFF FF5F-FFF FF6F-FFF FF7F-FFF		BIOS4 data space for SPI and LPC
FF80-0000 FF88-0000 FF90-0000 FF98-0000 FFA0-0000 FFA8-0000 FFB0-0000 FFB8-0000	FF87-FFFF FF8F-FFFF FF97-FFFF FF9F-FFFF FFA7-FFFF FFAF-FFFF FFB7-FFFF FFBF-FFFF		BIOS3 feature space for LPC
FFC0-0000	FFF7-FFFF		BIOS3 data space for SPI and LPC
FFF8-0000	FFFB-FFFF		BIOS2 data space for SPI and LPC
FFF0-0000	FFFF-FFFF		BIOS – data space for SPI and LPC
4Gb to TOUUD – High DRAM Window			
1_000-000	TOUUD-1		High main memory. Top of Upper Usable DRAM
TOUUD to 1024 GB – High MMIO			
TOUUD	1024 GB		High MMIO (64-bit MMIO)

[1] legacy support is not validated by Intel

10.3. I/O Address Map

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

Table 22: Designated I/O Port Address Ranges

I/O Address Range (hex)	General Usage	Project Usage
020-021 024-025 028-029 02C-02D	Interrupt Controller (8259 PIC)	Interrupt Controller
02E-02F	LPC	LPC
030-031	Interrupt Controller (8259 PIC)	Interrupt Controller

I/O Address Range (hex)	General Usage	Project Usage
034-035 038-039 03C-03D		
040 042-043	Interrupt Timer (8252 Timer)	Timer/Counter
04E-04F	LPC Controller	LPC Controller
050 052-053	Interrupt Timer (8252 Timer)	Timer/Counter
060	PS2 Legacy Keyboard/ Mouse	PS2 Legacy Keyboard/ Mouse
061	NMI Controller	NMI Controller
062	LPC	LPC
063	NMI Controller	NMI Controller
064	PS2 Legacy Keyboard/ Mouse	PS2 Legacy Keyboard/ Mouse
065	NMI Controller	NMI Controller
066	LPC	LPC
067	NMI Controller	NMI Controller
070	CPU Interface, RTC, Power Management Controller	CPU Interface, RTC, Power Management Controller
071-077	RTC Controller	RTC Controller
080 084-086 088 08C-08E	LPC or PCIe Root Port	LPC or PCIe Root Port
090	LPC	LPC
092	P2SB->ITSS CPU I/F	P2SB->ITSS CPU I/F
094-096 098 09C-09E	LPC	LPC
0A0-0A1 0A4- 0A5 0A8- 0A9 0AC-0AD 0B0- 0B1	Interrupt Controller (8259 PIC)	Interrupt Controller
0B2-0B3	Power Management SMI	Power Management SMI
0B4-0B5 0B8-0B9 0BC-0BD	Interrupt Controller (8259 PIC)	Interrupt Controller
200-20F 220-22F 238-23F 278-27F 2E8-2EF 2F8-2FF	LPC	LPC
2F8-2FF	COM2 (Fabric)	Serial Port COM2

I/O Address Range (hex)	General Usage	Project Usage
338-33F 370-375 377-37F	LPC	LPC
3B0-3B8	Can be routed to PCIe bridge whem BCTL.VGAE ser(fabric)	Can be routed to PCIe bridge whem BCTL.VGAE ser(fabric)
3BC-3BE	LPC	LPC
3C0-3DF	Routed to PCIe bridge (fabric)	Routed to PCIe bridge (fabric)
3E8-3F5 3F7-3FF	LPC	LPC
3F8-3FF	COM1 (Fabric)	Serial Port COM1
4D0-4D1	Interrupt Controller (ITSS Interrupt)	Interrupt Controller
678-67F 778-77F 7BC-7BE	LPC	LPC
A80-A81	Kontron CPLD control + Data port	
CF8	Access to confiruration registers	PCI configuration address
CF9	Software generated reset	Reset control
CFC	Access to confiruration registers	PCI Configuration data

Other PCI device I/O addresses are allocated dynamically and not listed here. For more information on how to determine I/O address usage, refer to the OS documentation.

10.4. Peripheral Component Interconnect (PCI) Devices

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

10.5. I2C Bus

The following table provides the I2C address for devices connected the I2C Bus.

Table 23: I2C Bus Port Addresses

I2C Address (hex)	Part	I2C Bus
	Embedded controller FPGA	I2C_EXT
A0h	COMe Module EEPROM	I2C_EXT
58h	5ECO Circuit	I2C_EXT
var.	COMexpress connector	I2C_EXT
(AEh)	(carrier EEprom)	I2C_EXT

10.6. System Management (SMBus)

The 8-bit SMBus address uses the LSB (Bit 0) for the direction of the device.

- Bit0 = 0 defines the write address
- Bit0 = 1 defines the read address

The 8-bit address listed below shows the write address for all devices. The7-bit SMBus address shows the device address without Bit0.

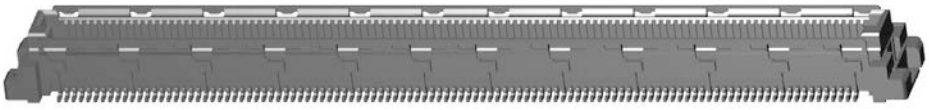
Table 24: SMBus Addresses

8-bit Address	7-bit Address	Device	SMBus
		SoC	SMB_LEG
A0h	50h	DDR4 SODIMM A	SMB_RAM
A4h	52h	DDR4 SODIMM B	SMB_RAM
A2h	51h	DDR4 SODIMM C	SMB_RAM
A6h	53h	DDR4 SODIMM D	SMB_RAM
var.	var.	XDP Connector	SMB_LEG
92h	49h	I210 GbE0 Controller	SMB_LEG
5Ch	2Eh	NCT7802Y HW Monitor	SMB_S0
var.	Var.	COMexpress connector	SMB

11/ COMe Connector

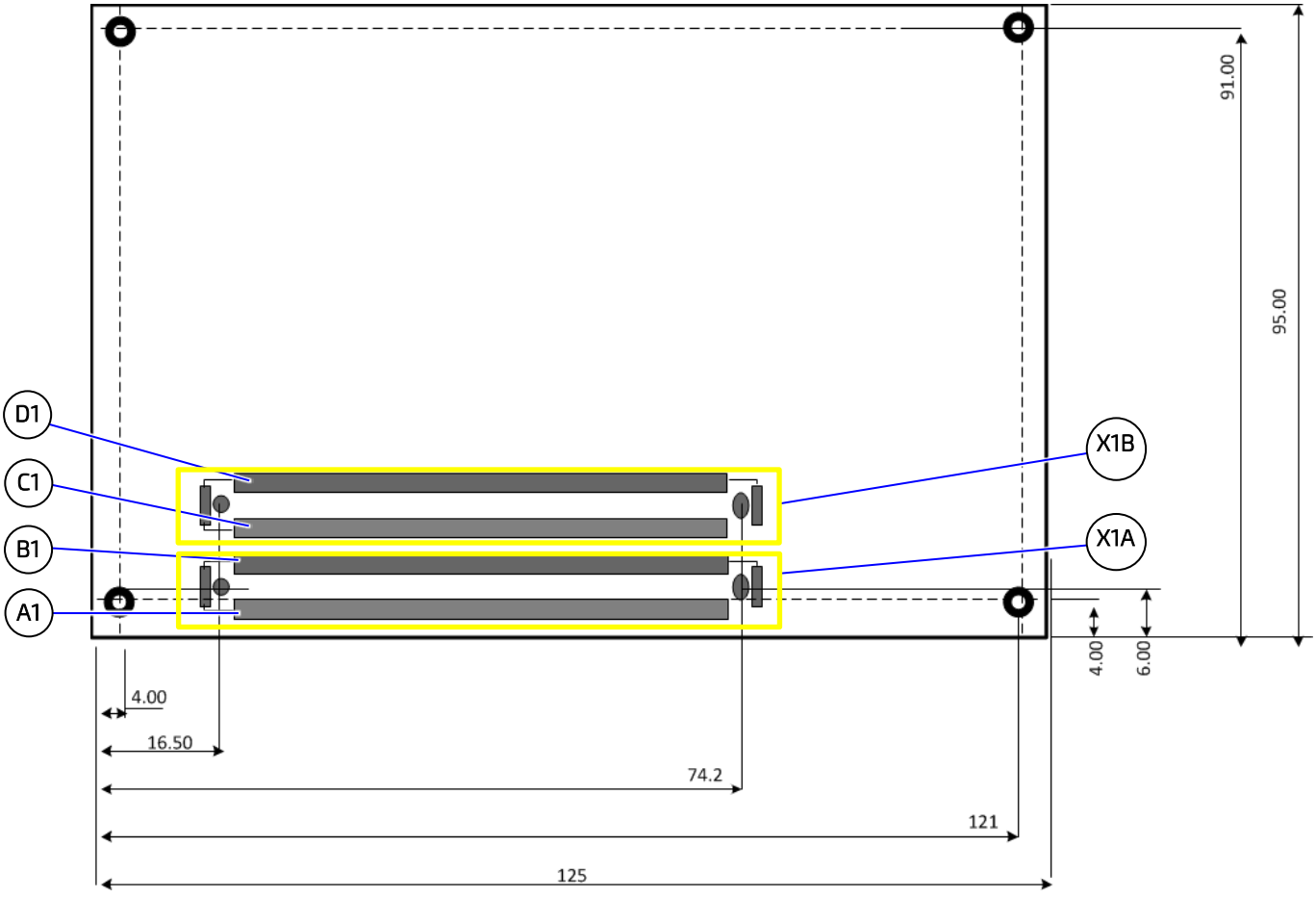
The COMe-bDV7 is a COM Express® basic module containing two 220-pin connectors; each with two rows called row A & row B on the primary connector and row C & row D on the secondary connector.

Figure 8: COMe Connector with 220 pins



The following figure is a view from the bottom of the module showing the position of interface connectors X1A and indicating the location of pin A1, B1, C1 and D1.

Figure 9: X1A and X1B COMe Interface Connectors



11.1. X1A and X1B COMe Interface Connector Signals

For a description of the terms used within the pin assignment tables, see Table 25: General Signal Description below or Appendix A, List of Acronyms. If a more detailed pin assignment description is required, refer to the PICMG Specification COMe Rev 3.0 Type 7 standard.

The information provided under type, module terminations and comments is complimentary to the COM.0 Rev 3.0 Type 7 standard. For more information, contact Kontron Support.

Table 25: General Signal Description

Type	Description	Type	Description
NC	Not Connected (on this product)	**O-1,8**	1.8 V Output
I/O-3,3	Bi-directional 3.3 V I/O-Signal	**O-3,3**	3.3 V Output
I/O-5T	Bi-dir. 3.3 V I/O (5 V Tolerance)	**O-5**	5 V Output
I/O-5	Bi-directional 5V I/O-Signal	**DP-I/O**	Differential Pair Input/Output
I-3,3	3.3 V Input	**DP-I**	Differential Pair Input
I/OD	Bi-directional Input/Output Open Drain	**DP-O**	Differential Pair Output
I-5T	3.3 V Input (5 V Tolerance)	**PU**	Pull-up Resistor
OA	Output Analog	**PWR**	Power Connection
OD	Output Open Drain	**+ and -**	Differential Pair

NOTICE

To protect external power lines of peripheral devices, make sure that the wires have the right diameter to withstand the maximum available current.

The enclosure of the peripheral device fulfills the fire-protection requirements of IEC/EN60950.

11.2. COMe Connector (X1A and X1B) Pin Assignment

The following tables list the pin assignment of the two 220-pin connectors and both rows.

- Table 26: X1A Connector Pin Assignment Row (A1-A110)
- Table 27: X1A Connector Pin Assignment Row (B1-B110)
- Table 28: X1B Connector Pin Assignment Row (C1-C110)
- Table 29: X1B Connector Pin Assignment Row (D1-D110)

11.2.1. Connector X1A Row A1 - A110

Table 26: X1A Connector Pin Assignment Row (A1-A110)

Pin	COMe Signal	Description	Type	Termination	Comment
A1	GND	Power Ground	PWR GND		
A2	GBE0_MDI3-	Ethernet Media Dependent Interface 3 -	DP-I/O		
A3	GBE0_MDI3+	Ethernet Media Dependent Interface 3 +			
A4	GBE0_LINK100#	Ethernet Speed LED	OD		
A5	GBE0_LINK1000#	Ethernet Speed LED	OD		
A6	GBE0_MDI2-	Ethernet Media Dependent Interface 2 -	DP-I/O		
A7	GBE0_MDI2+	Ethernet Media Dependent Interface 2 +			
A8	GBE0_LINK#	LAN Link LED	OD		
A9	GBE0_MDI1-	Ethernet Media Dependent Interface 1 -	DP-I/O		
A10	GBE0_MDI1+	Ethernet Media Dependent Interface 1 +			
A11	GND	Power Ground	PWR GND		
A12	GBE0_MDI0-	Ethernet Media Dependent Interface 0 -	DP-I/O		
A13	GBE0_MDI0+	Ethernet Media Dependent Interface 0 +			
A14	GBE0_CTREF	Center Tab Reference Voltage	REF		1 µF/25 V
A15	SUS_S3#	Suspend To RAM (or deeper) Indicator	O-3.3		
A16	SATA0_TX+	SATA Transmit Pair 0 +	DP-O	AC Coupled on Module	
A17	SATA0_TX-	SATA Transmit Pair 0 -			
A18	SUS_S4#	Suspend To Disk (or deeper) Indicator	O-3.3		
A19	SATA0_RX+	SATA Receive Pair 0 +	DP-I	AC Coupled on Module	
A20	SATA0_RX-	SATA Receive Pair 0 -			
A21	GND	Power Ground	PWR GND		
A22	PCIE_TX15+	PCI Express Lane 15 Transmit +	DP-O	AC Coupled on Module	
A23	PCIE_TX15-	PCI Express Lane 15 Transmit -			
A24	SUS_S5#	Soft Off Indicator	O-3.3		
A25	PCIE_TX14+	PCI Express Lane 14 Transmit +	DP-O	AC Coupled on Module	
A26	PCIE_TX14-	PCI Express Lane 14 Transmit -			
A27	BATLOW#	Battery Low	I-3.3	PU 10k 3.3V (S5)	Assertion prevents wake from S3-S5 state
A28	ATA_ACT#	Serial ATA activity LED	I/O-3.3	PU 10k 3.3V (S0)	Can sink 15 mA
A29	RSVD	Reserved for future use	NC		
A30	RSVD	Reserved for future use	NC		
A31	GND	Power Ground	PWR GND		
A32	RSVD	Reserved for future use	NC		
A33	RSVD	Reserved for future use	NC		
A34	BIOS_DIS0#/ESPI_SAFS	BIOS Selection Strap 0	I-3.3	PU 10k 3.3V (S5)	
A35	THRMTRIP#	Thermal Trip	O-3.3		Thermal trip event transition to S5 indicator
A36	PCIE_TX13+	PCI Express Lane 13 Transmit +	NC		
A37	PCIE_TX13-	PCI Express Lane 13 Transmit -	NC		
A38	GND	Power Ground	PWR GND		
A39	PCIE_TX12+	PCI Express Lane 12 Transmit +	NC		
A40	PCIE_TX12-	PCI Express Lane 12 Transmit -	NC		
A41	GND	Power Ground	PWR GND		
A42	USB2-	USB 2.0 Data Pair Port 2 –	DP-I/O		
A43	USB2+	USB 2.0 Data Pair Port 2 +			

Pin	COMe Signal	Description	Type	Termination	Comment
A44	USB_2_3_OC#	USB Overcurrent Indicator Port 2/3	I-3.3	PU 10k 3.3V (S5)	
A45	USB0-	USB 2.0 Data Pair Port 0 –	DP-I/O		
A46	USB0+	USB 2.0 Data Pair Port 0 +			
A47	VCC_RTC	Real-Time Clock Circuit Power Input	PWR 3 V		Voltage range 2.0 V to 3.3 V (3.0 V Nominal)
A48	RSVD	Reserved for future use	nc		
A49	GBE0_SDP	Gigabit Eth. Controller 0 Software-Definable Pin.	I/O-3.3 (S5)		
A50	LPC_SERIRQ/ESPI_CS1#	Serial Interrupt Request	I/OD-3.3	PU 8k2 3.3V (S0)	
A51	GND	Power Ground	PWR GND		
A52	PCIE_TX5+	PCI Express Lane 5 Transmit +	DP-O	AC Coupled on Module	
A53	PCIE_TX5-	PCI Express Lane 5 Transmit -			
A54	GPI0	General Purpose Input 0	I-3.3	PU 100k 3.3V (S0)	
A55	PCIE_TX4+	PCI Express Lane 4 Transmit +	DP-O	AC Coupled on Module	
A56	PCIE_TX4-	PCI Express Lane 4 Transmit -			
A57	GND	Power Ground	PWR GND		
A58	PCIE_TX3+	PCI Express Lane 3 Transmit +	DP-O	AC Coupled on Module	
A59	PCIE_TX3-	PCI Express Lane 3 Transmit -			
A60	GND	Power Ground	PWR GND		
A61	PCIE_TX2+	PCI Express Lane 2 Transmit +	DP-O	AC Coupled on Module	
A62	PCIE_TX2-	PCI Express Lane 2 Transmit -			
A63	GPI1	General Purpose Input 1	I-3.3	PU 100k 3.3 V (S0)	
A64	PCIE_TX1+	PCI Express Lane 1 Transmit +	DP-O	AC Coupled on Module	
A65	PCIE_TX1-	PCI Express Lane 1 Transmit -			
A66	GND	Power Ground	PWR GND		
A67	GPI2	General Purpose Input 2	I-3.3	PU 100k 3.3V (S0)	
A68	PCIE_TX0+	PCI Express Lane 0 Transmit +	DP-O	AC Coupled on Module	
A69	PCIE_TX0-	PCI Express Lane 0 Transmit -			
A70	GND	Power Ground	PWR GND		
A71	PCIE_TX8+	PCI Express Lane 8 Transmit +	DP-O	AC Coupled on Module	
A72	PCIE_TX8-	PCI Express Lane 8 Transmit -			
A73	GND	Power Ground	PWR GND		
A74	PCIE_TX9+	PCI Express Lane 9 Transmit +	DP-O	AC Coupled on Module	
A75	PCIE_TX9-	PCI Express Lane 9 Transmit -	DP-O		
A76	GND	Power Ground	PWR GND		
A77	PCIE_TX10+	PCI Express Lane 10 Transmit +	DP-O	AC Coupled on Module	
A78	PCIE_TX10-	PCI Express Lane 10 Transmit -	DP-O		
A79	GND	Power Ground	PWR GND		
A80	GND	Power Ground	PWR GND		
A81	PCIE_TX11+	PCI Express Lane 11 Transmit +	DP-O	AC Coupled on Module	
A82	PCIE_TX11-	PCI Express Lane 11 Transmit -			
A83	GND	Power Ground	PWR GND		
A84	NCSI_TX_EN	NC-SI Transmit enable	I-3.3 (S5)	PD 10k	
A85	GPI3	General Purpose Input 3	I-3.3	PU 100k 3.3V (S0)	
A86	RSVD	Reserved for future use	N		
A87	RSVD	Reserved for future use	NC		
A88	PCIE_CK_REF+	Reference PCI Express Clock +	DP-O		100 MHz
A89	PCIE_CK_REF-	Reference PCI Express Clock -			

Pin	COMe Signal	Description	Type	Termination	Comment
A90	GND	Power Ground	PWR GND		
A91	SPI_POWER	3.3V Power Output Pin for external SPI flash	O-3.3		100 mA maximum
A92	SPI_MISO	SPI Master IN Slave OUT	I-3.3	0 R	
A93	GPO0	General Purpose Output 0	O-3.3	PD 100k	
A94	SPI_CLK	SPI Clock	O-3.3	0 R	
A95	SPI_MOSI	SPI Master Out Slave In	O-3.3	0 R	
A96	TPM_PP	TPM Physical Presence	I-3.3	PD 10k	
A97	TYPE10#	Indicates TYPE10# to carrier board	nc		
A98	SER0_TX	Serial Port 0 TXD	O-3.3		20 V protection circuit implemented on-module, PD on carrier board needed for proper operation.
A99	SER0_RX	Serial Port 0 RXD	I-5T	PU 10k	20 V protection circuit implemented on-module.
A100	GND	Power Ground	PWR GND		
A101	SER1_TX	Serial Port 1 TXD	O-3.3		20 V protection circuit implemented on-module, PD on carrier board needed for proper operation.
A102	SER1_RX	Serial Port 1 RXD	I-5T	PU 10k	20 V protection circuit implemented on-module.
A103	LID#	LID Switch Input	I-3.3	PU 47k 3.3V (S5)	
A104	VCC_12V	Main Input Voltage	PWR		
A105	VCC_12V				
A106	VCC_12V				
A107	VCC_12V				
A108	VCC_12V				
A109	VCC_12V				
A110	GND	Power Ground	PWR GND		

11.2.2. Connector X1A Row B1 - B100

Table 27: X1A Connector Pin Assignment Row (B1-B110)

Pin	COMe Signal	Description	Type	Termination	Comment
B1	GND	Power Ground	PWR GND		
B2	GBE0_ACT#	Ethernet Activity LED	OD		
B3	LPC_FRAME#/ESPI_CS0#	LPC Frame Indicator	O-3.3		
B4	LPC_AD0/ESPI_IO_0	LPC Multiplexed Command, Address & Data 0	I/O-3.3		
B5	LPC_AD1/ESPI_IO_1	LPC Multiplexed Command, Address & Data 1			
B6	LPC_AD2/ESPI_IO_2	LPC Multiplexed Command, Address & Data 2			
B7	LPC_AD3/ESPI_IO_3	LPC Multiplexed Command, Address & Data 3			
B8	LPC_DRQ0#/ESPI_ALERT0#	LPC Serial DMA/Master Request 0	NC		Not supported
B9	LPC_DRQ1#/ESPI_ALERT1#	LPC Serial DMA/Master Request 1	NC		Not supported
B10	LPC_CLK/ESPI_CK	24MHz LPC clock	O-3.3		24MHz (LPC clock generated from Soc)
B11	GND	Power Ground	PWR GND		
B12	PWRBTN#	Power Button	I-3.3	PU 10k 3.3V (S5eco)	
B13	SMB_CK	SMBUS Clock	O-3.3	PU 2k2 3.3V (S5)	
B14	SMB_DAT	SMBUS Data	I/O-3.3	PU 2k2 3.3V (S5)	
B15	SMB_ALERT#	SMBUS Alert	I/O-3.3	PU 2k2 3.3V (S5)	
B16	SATA1_TX+	SATA 1 Transmit Pair +	DP-O	AC Coupled on Module	
B17	SATA1_TX-	SATA 1 Transmit Pair -			
B18	SUS_STAT#	Suspend Status	O-3.3		
B19	SATA1_RX+	SATA 1 Receive Pair +	DP-I	AC Coupled on Module	
B20	SATA1_RX-	SATA 1 Receive Pair -			
B21	GND	Power Ground	PWR GND		
B22	PCIE_RX15+	PCI Express Lane 15 Receive +	DP-I		
B23	PCIE_RX15-	PCI Express Lane 15 Receive -			
B24	PWR_OK	Power OK	I-3.3	PU 1.1M (S5)	
B25	PCIE_TX14+	PCI Express Lane 14 Receive +	DP-I		
B26	PCIE_TX14-	PCI Express Lane 14 Receive -			
B27	WDT	Watch Dog Time-Out event	O-3.3	PD 10K	
B28	RSVD	Reserved for future use	NC		
B29	RSVD	Reserved for future use			
B30	RSVD	Reserved for future use			
B31	GND	Power Ground	PWR GND		
B32	SPKR	Speaker	NC		
B33	I2C_CK	I2C Clock	O-3.3	PU 2k2 3.3V (S5)	
B34	I2C_DAT	I2C Data	I/O-3.3	PU 2k2 3.3V (S5)	
B35	THRM#	Over Temperature Input	I-3.3	PU 10k 3.3V	
B36	PCIE_RX13+	PCI Express Lane 13 Receive +	DP-I		
B37	PCIE_RX13-	PCI Express Lane 13 Receive -			
B38	GND	Power Ground	PWR GND		
B39	PCIE_RX12+	PCI Express Lane 12 Receive +	DP-I		
B40	PCIE_RX12-	PCI Express Lane 12 Receive -			

Pin	COMe Signal	Description	Type	Termination	Comment
B41	GND	Power Ground	PWR GND		
B42	USB3-	USB 2.0 Data Pair Port 3 –	DP-I/O		
B43	USB3+	USB 2.0 Data Pair Port 3 +			
B44	USB_0_1_OC#	USB Overcurrent Indicator Port 0/1	I-3.3	PU 10k 3.3V (S5)	
B45	USB1-	USB 2.0 Data Pair Port 1 –	DP-I/O		
B46	USB1+	USB 2.0 Data Pair Port 1 +			
B47	ESPI_EN#	LPC/eSPI mode selection	NC	PU 20K (S5)	Not supported
B48	USB0_HOST_PRSNT	USB host presence on USB0	NC	PU 20K (S5)	Not supported
B49	SYS_RESET#	Reset Button Input	I-3.3	PU 10k 3.3V (S5)	
B50	CB_RESET#	Carrier Board Reset	O-3.3		
B51	GND	Power Ground	PWR GND		
B52	PCIE_RX5+	PCI Express Lane 5 Receive +	DP-I		
B53	PCIE_RX5-	PCI Express Lane 5 Receive -			
B54	GPO1	General Purpose Output 1	O-3.3	PD 100k	
B55	PCIE_RX4+	PCI Express Lane 4 Receive +	DP-I		
B56	PCIE_RX4-	PCI Express Lane 4 Receive -			
B57	GPO2	General Purpose Output 2	O-3.3	PD 100k	
B58	PCIE_RX3+	PCI Express Lane 3 Receive +	DP-I		
B59	PCIE_RX3-	PCI Express Lane 3 Receive -			
B60	GND	Power Ground	PWR GND		
B61	PCIE_RX2+	PCI Express Lane 2 Receive +	DP-I		
B62	PCIE_RX2-	PCI Express Lane 2 Receive -			
B63	GPO3	General Purpose Output 3	O-3.3	PD 100k	
B64	PCIE_RX1+	PCI Express Lane 1 Receive +	DP-I		
B65	PCIE_RX1-	PCI Express Lane 1 Receive -			
B66	WAKE0#	PCI Express Wake Up Event	I-3.3	PU 10k 3.3V (S5)	
B67	WAKE1#	General Purpose Wake Up Event	I-3.3	PU 10k 3.3V (S5)	
B68	PCIE_RX0+	PCI Express Lane 0 Receive +	DP-I		
B69	PCIE_RX0-	PCI Express Lane 0 Receive -			
B70	GND	Power Ground	PWR GND		
B71	PCIE_RX8+	PCI Express Lane 8 Receive +	DP-I		
B72	PCIE_RX8-	PCI Express Lane 8 Receive -	DP-I		
B73	GND	Power Ground	PWR GND		
B74	PCIE_RX9+	PCI Express Lane 9 Receive +	DP-I		
B75	PCIE_RX9-	PCI Express Lane 9 Receive -	DP-I		
B76	GND	Power Ground	PWR GND		
B77	PCIE_RX10+	PCI Express Lane 10 Receive +	DP-I		
B78	PCIE_RX10-	PCI Express Lane 10 Receive -	DP-I		
B79	GND	Power Ground	PWR GND		
B80	GND	Power Ground	PWR GND		
B81	PCIE_RX11+	PCI Express Lane 11 Receive +	DP-I		
B82	PCIE_RX11-	PCI Express Lane 11 Receive -	DP-I		
B83	GND	Power Ground	PWR GND		
B84	VCC_5V_SBY	5V Standby	PWR 5V (S5)		optional (not necessary in single supply mode)
B85	VCC_5V_SBY	5V Standby			
B86	VCC_5V_SBY	5V Standby			
B87	VCC_5V_SBY	5V Standby			
B88	BIOS_DIS1#	BIOS Selection Strap 1	I-3.3	PU 10k 3.3V (S5)	

Pin	COMe Signal	Description	Type	Termination	Comment
B89	NCSI_RX_ER	NC-SI Receive error	NC	PD 10K	Optional signal and not used.
B90	GND	Power Ground	PWR GND		
B91	NCSI_CLK_IN	NC-SI Clock	I-3.3	PD 10k	
B92	NCSI_RXD1	NC-SI Receive Data	O-3.3		
B93	NCSI_RXD0	NC-SI Receive Data	O-3.3		
B94	NCSI_CRS_DV	NC-SI Carrier Sense/Receive Data Valid	O-3.3		
B95	NCSI_TXD1	NC-SI Transmit Data	I-3.3	PD 10k	
B96	NCSI_TXD0	NC-SI Transmit Data	I-3.3	PD 10k	
B97	SPI_CS#	SPI Chip Select	O-3.3		
B98	NCSI_ARB_IN	NC-SI hardware arbitration input	I-3.3	PU 10k (S5)	
B99	NCSI_ARB_OUT	NC-SI hardware arbitration output	O-3.3		
B100	GND	Power Ground	PWR GND		
B101	FAN_PWMOUT	Fan PWM Output	O-3.3		20V protection circuit implemented on module, PD on carrier board needed for proper operation
B102	FAN_TACHIN	Fan Tach Input	I-3.3	PU 47k 3.3V (S0)	20V protection circuit implemented on module
B103	SLEEP#	Sleep Button Input	I-3.3	PU 47k 3.3V (S5)	20V protection circuit implemented on module
B104	VCC_12V	Main Input Voltage	PWR		
B105	VCC_12V				
B106	VCC_12V				
B107	VCC_12V				
B108	VCC_12V				
B109	VCC_12V				
B110	GND	Power Ground	PWR GND		

11.2.3. Connector X1B Row C1 - C110

Table 28: X1B Connector Pin Assignment Row (C1-C110)

Pin	COMe Signal	Description	Type	Termination	Comment
C1	GND	Power Ground	PWR GND		
C2	GND				
C3	USB_SSRX0-	USB Super Speed Receive – (0)	DP-I		
C4	USB_SSRX0+	USB Super Speed Receive + (0)			
C5	GND	Power Ground	PWR GND		
C6	USB_SSRX1-	USB Super Speed Receive – (1)	DP-I		
C7	USB_SSRX1+	USB Super Speed Receive + (1)			
C8	GND	Power Ground	PWR GND		
C9	USB_SSRX2-	USB Super Speed Receive – (2)	DP-I		
C10	USB_SSRX2+	USB Super Speed Receive + (2)			
C11	GND	Power Ground	PWR GND		
C12	USB_SSRX3-	USB Super Speed Receive – (3)	DP-I		
C13	USB_SSRX3+	USB Super Speed Receive + (3)			
C14	GND	Power Ground	PWR GND		
C15	10G_PHY_MDC_SCL3	Management I2C Clock for external PHY	O/OD-3.3	PU 2k2 3.3V (S5)	
C16	10G_PHY_MDC_SCL2	Management I2C Clock for external PHY			
C17	10G_SDP2	Software-Definable Pin	I/O-3.3		
C18	GND	Power Ground	PWR GND		
C19	PCIE_RX6+	PCI Express Lane 6 Receive +	DP-I		
C20	PCIE_RX6-	PCI Express Lane 6 Receive -			
C21	GND	Power Ground	PWR GND		
C22	PCIE_RX7+	PCI Express Lane 7 Receive +	DP-I		
C23	PCIE_RX7-	PCI Express Lane 7 Receive -			
C24	10G_INT2	Interrupt From copper PHY or optical SFP Module	I-3.3	PU 2k2 3.3V (S5)	
C25	GND	Power Ground	PWR GND		
C26	10G_KR_RX3+	10GBASE-KR receive differential pair +	DP-I	AC Coupled on Module	
C27	10G_KR_RX3-	10GBASE-KR receive differential pair -			
C28	GND	Power Ground	PWR GND		
C29	10G_KR_RX2+	10GBASE-KR receive differential pair +	DP-I	AC Coupled on Module	
C30	10G_KR_RX2-	10GBASE-KR receive differential pair -			
C31	GND	Power Ground	PWR GND		
C32	10G_SFP_SDA3	Management I2C Data for optical SFP Module	I/O-3.3	PU 2k2 3.3V (S5)	
C33	10G_SFP_SDA2	Management I2C Data for optical SFP Module			
C34	10G_PHY_RST_23	Reset of optical PHY on ports 2 and 3	O-3.3		
C35	10G_PHY_RST_01	Reset of optical PHY on ports 0 and 1			
C36	10G_LED_SDA	I2C Data to transfer LED signals or MDIO of opt. PHY	I/O-3.3	PU 2k2 3.3V (S5)	
C37	10G_LED_SCL	I2C Clock to transfer LED signals or MDIO of opt. PHY	O-3.3	PU 2k2 3.3V (S5)	
C38	10G_SFP_SDA1	Management I2C Data for optical SFP Module	I/O-3.3	PU 2k2 3.3V (S5)	
C39	10G_SFP_SDA0	Management I2C Data for optical SFP Module	I/O-3.3	PU 2k2 3.3V (S5)	
C40	10G_SDP0	Software-Definable Pin	I/O-3.3		
C41	GND	Power Ground	PWR GND		
C42	10G_KR_RX1+	10GBASE-KR receive differential pair +	DP-I	AC Coupled on Module	
C43	10G_KR_RX1-	10GBASE-KR receive differential pair +			
C44	GND	Power Ground	PWR GND		

Pin	COMe Signal	Description	Type	Termination	Comment
C45	10G_PHY_MDC_SCL1	Management I2C Clock for external PHY	O/OD-3.3	PU 2k2 3.3V (S5)	
C46	10G_PHY_MDC_SCL0	Management I2C Clock for external PHY			
C47	10G_INT0	Interrupt From copper PHY or optical SFP Module	I-3.3	PU 2k2 3.3V (S5)	
C48	GND	Power Ground	PWR GND		
C49	10G_KR_RX0+	10GBASE-KR receive differential pair +	DP-I	AC Coupled on Module	
C50	10G_KR_RX0-	10GBASE-KR receive differential pair +			
C51	GND	Power Ground	PWR GND		
C52	PCIE_RX16+	PCI Express Lane 16 Receive +	DP-I		
C53	PCIE_RX16-	PCI Express Lane 16 Receive -			
C54	TYPE0#	GND for type 7 module	GND		
C55	PCIE_RX17+	PCI Express Lane 17 Receive +	DP-I		
C56	PCIE_RX17-	PCI Express Lane 17 Receive -			
C57	TYPE1#	NC for type 7 module	NC		
C58	PCIE_RX18+	PCI Express Lane 18 Receive +	DP-I		
C59	PCIE_RX18-	PCI Express Lane 18 Receive -			
C60	GND	Power Ground	PWR GND		
C61	PCIE_RX19+	PCI Express Lane 19 Receive +	DP-I		
C62	PCIE_RX19-	PCI Express Lane 19 Receive -			
C63	RSVD	Reserved for future use	NC		
C64	RSVD	Reserved for future use			
C65	PCIE_RX20+	PCI Express Lane 20 Receive +	DP-I		
C66	PCIE_RX20-	PCI Express Lane 20 Receive -			
C67	RAPID_SHUTDOWN	Trigger for Rapid Shutdown	I-5.0	PD 100K	
C68	PCIE_RX21+	PCI Express Lane 21 Receive +	DP-I		
C69	PCIE_RX21-	PCI Express Lane 21 Receive -			
C70	GND	Power Ground	PWR GND		
C71	PCIE_RX22+	PCI Express Lane 22 Receive +	DP-I		
C72	PCIE_RX22-	PCI Express Lane 22 Receive -			
C73	GND	Power Ground	PWR GND		
C74	PCIE_RX23+	PCI Express Lane 23 Receive +	DP-I		
C75	PCIE_RX23-	PCI Express Lane 23 Receive -			
C76	GND	Power Ground	PWR GND		
C77	RSVD	Reserved for future use	NC		
C78	PCIE_RX24+	PCI Express Lane 24 Receive +	DP-I		
C79	PCIE_RX24-	PCI Express Lane 24 Receive -			
C80	GND	Power Ground	PWR GND		
C81	PCIE_RX25+	PCI Express Lane 25 Receive +	DP-I		
C82	PCIE_RX25-	PCI Express Lane 25 Receive -	DP-I		
C83	RSVD	Reserved for future use	NC		
C84	GND	Power Ground	PWR GND		
C85	PCIE_RX26+	PCI Express Lane 26 Receive +	DP-I		
C86	PCIE_RX26-	PCI Express Lane 26 Receive -			
C87	GND	Power Ground	PWR GND		
C88	PCIE_RX27+	PCI Express Lane 27 Receive +	DP-I		
C89	PCIE_RX27-	PCI Express Lane 27 Receive -			
C90	GND	Power Ground	PWR GND		
C91	PCIE_RX28+	PCI Express Lane 28 Receive +	DP-I		
C92	PCIE_RX28-	PCI Express Lane 28 Receive -			
C93	GND	Power Ground	PWR GND		
C94	PCIE_RX29+	PCI Express Lane 29 Receive +	DP-I		
C95	PCIE_RX29-	PCI Express Lane 29 Receive -			

Pin	COMe Signal	Description	Type	Termination	Comment
C96	GND	Power Ground	PWR GND		
C97	RSVD	Reserved for future use	NC		
C98	PCIE_RX30+	PCI Express Lane 30 Receive +	DP-I		
C99	PCIE_RX30-	PCI Express Lane 30 Receive -			
C100	GND	Power Ground	PWR GND		
C101	PCIE_RX31+	PCI Express Lane 31 Receive +	DP-I		
C102	PCIE_RX31-	PCI Express Lane 31 Receive -			
C103	GND	Power Ground	PWR GND		
C104	VCC_12V	Main Input Voltage	PWR		
C105	VCC_12V				
C106	VCC_12V				
C107	VCC_12V				
C108	VCC_12V				
C109	VCC_12V				
C110	GND	Power Ground	PWR GND		

11.2.4. Connector X1B Row D1 - D110

Table 29: X1B Connector Pin Assignment Row (D1-D110)

Pin	COMe Signal	Description	Type	Termination	Comment
D1	GND	Power Ground	PWR GND		
D2	GND	Power Ground			
D3	USB_SSTX0-	USB Super Speed Transmit – (0)	DP-O		
D4	USB_SSTX0+	USB Super Speed Transmit + (0)			
D5	GND	Power Ground	PWR GND		
D6	USB_SSTX1-	USB Super Speed Transmit – (1)	DP-O		
D7	USB_SSTX1+	USB Super Speed Transmit + (1)			
D8	GND	Power Ground	PWR GND		
D9	USB_SSTX2-	USB Super Speed Transmit – (2)	DP-O		
D10	USB_SSTX2+	USB Super Speed Transmit + (2)			
D11	GND	Power Ground	PWR GND		
D12	USB_SSTX3-	USB Super Speed Transmit – (3)	DP-O		
D13	USB_SSTX3+	USB Super Speed Transmit + (3)			
D14	GND	Power Ground	PWR GND		
D15	10G_PHY_MDIO_SDA3	Management I2C Data for external PHY	I/O-3.3	PU 2k2 3.3V (S5)	
D16	10G_PHY_MDIO_SDA2	Management I2C Data for external PHY			
D17	10G_SDP3	Software-Definable Pin	I/O-3.3		
D18	GND	Power Ground	PWR GND		
D19	PCIE_TX6+	PCI Express Lane 6 Transmit +	DP-O	AC Coupled on Module	
D20	PCIE_TX6-	PCI Express Lane 6 Transmit -			
D21	GND	Power Ground	PWR GND		
D22	PCIE_TX7+	PCI Express Lane 7 Transmit +	DP-O	AC Coupled on Module	
D23	PCIE_TX7-	PCI Express Lane 7 Transmit -			
D24	10G_INT3	Interrupt From copper PHY or optical SFP Module	I-3.3	PU 2k2 3.3V (S5)	
D25	GND	Power Ground	PWR GND		
D26	10G_KR_TX3+	10GBASE-KR transmit differential pair +	DP-O		
D27	10G_KR_TX3-	10GBASE-KR transmit differential pair -			
D28	GND	Power Ground	PWR GND		
D29	10G_KR_TX2+	10GBASE-KR transmit differential pair +	DP-O		
D30	10G_KR_TX2-	10GBASE-KR transmit differential pair -			
D31	GND	Power Ground	PWR GND		
D32	10G_SFP_SCL3	Management I2C Clock for optical SFP Module	I/O-3.3	PU 2k2 3.3V (S5)	
D33	10G_SFP_SCL2	Management I2C Clock for optical SFP Module			
D34	10G_PHY_CAP_23	PHY on ports 2 and 3 mode capability – I2C or MDIO	I-3.3	PU 10k 3.3V (S5)	
D35	10G_PHY_CAP_01	PHY on ports 0 and 1 mode capability – I2C or MDIO	I-3.3	PU 10k 3.3V (S5)	
D36	RSVD	Reserved for future use	NC		
D37	RSVD	Reserved for future use			
D38	10G_SFP_SCL1	Management I2C Clock for optical SFP Module	I/O-3.3	PU 2k2 3.3V (S5)	
D39	10G_SFP_SCL0	Management I2C Clock for optical SFP Module	I/O-3.3	PU 2k2 3.3V (S5)	
D40	10G_SDP1	Software-Definable Pin	I/O-3.3		
D41	GND	Power Ground	PWR GND		
D42	10G_KR_TX1+	10GBASE-KR transmit differential pair +	DP-O		
D43	10G_KR_TX1-	10GBASE-KR transmit differential pair -			
D44	GND	Power Ground	PWR GND		

Pin	COMe Signal	Description	Type	Termination	Comment
D45	10G_PHY_MDIO_SDA1	Management I2C Data for external PHY	I/O-3.3	PU 2k2 3.3V (S5)	
D46	10G_PHY_MDIO_SDA0	Management I2C Data for external PHY	I/O-3.3	PU 2k2 3.3V (S5)	
D47	10G_INT1	Interrupt From copper PHY or optical SFP Module	I-3.3	PU 2k2 3.3V (S5)	
D48	GND	Power Ground	PWR GND		
D49	10G_KR_TX0+	10GBASE-KR transmit differential pair +	DP-O		
D50	10G_KR_TX0-	10GBASE-KR transmit differential pair			
D51	GND	Power Ground	PWR GND		
D52	PCIE_TX16+	PCI Express Lane 16 Transmit +	DP-O	AC Coupled on Module	
D53	PCIE_TX16-	PCI Express Lane 16 Transmit -			
D54	RSVD	Reserved for future use	NC		
D55	PCIE_TX17+	PCI Express Lane 17 Transmit +	DP-O	AC Coupled on Module	
D56	PCIE_TX17-	PCI Express Lane 17 Transmit -			
D57	TYPE2#	GND for type 7 module	GND		
D58	PCIE_TX18+	PCI Express Lane 18 Transmit +	DP-O	AC Coupled on Module	
D59	PCIE_TX18-	PCI Express Lane 18 Transmit -			
D60	GND	Power Ground	PWR GND		
D61	PCIE_TX19+	PCI Express Lane 19 Transmit +	DP-O	AC Coupled on Module	
D62	PCIE_TX19-	PCI Express Lane 19 Transmit -			
D63	RSVD	Reserved for future use	NC		
D64	RSVD	Reserved for future use			
D65	PCIE_TX20+	PCI Express Lane 20 Transmit +	DP-O	AC Coupled on Module	
D66	PCIE_TX20-	PCI Express Lane 20 Transmit -			
D67	GND	Power Ground	PWR GND		
D68	PCIE_TX21+	PCI Express Lane 21 Transmit +	DP-O	AC Coupled on Module	
D69	PCIE_TX21-	PCI Express Lane 21 Transmit -			
D70	GND	Power Ground	PWR GND		
D71	PCIE_TX22+	PCI Express Lane 22 Transmit +	DP-O	AC Coupled on Module	
D72	PCIE_TX22-	PCI Express Lane 22 Transmit -			
D73	GND	Power Ground	PWR GND		
D74	PCIE_TX23+	PCI Express Lane 23 Transmit +	DP-O	AC Coupled on Module	
D75	PCIE_TX23-	PCI Express Lane 23 Transmit -			
D76	GND	Power Ground	PWR GND		
D77	RSVD	Reserved for future use	NC		
D78	PCIE_TX24+	PCI Express Lane 24 Transmit +	DP-O	AC Coupled on Module	
D79	PCIE_TX24-	PCI Express Lane 24 Transmit -			
D80	GND	Power Ground	PWR GND		
D81	PCIE_TX25+	PCI Express Lane 25 Transmit +	DP-O	AC Coupled on Module	
D82	PCIE_TX25-	PCI Express Lane 25 Transmit -			
D83	RSVD	Reserved for future use	NC		
D84	GND	Power Ground	PWR GND		
D85	PCIE_TX26+	PCI Express Lane 26 Transmit +	DP-O	AC Coupled on Module	
D86	PCIE_TX26-	PCI Express Lane 26 Transmit -			
D87	GND	Power Ground	PWR GND		
D88	PCIE_TX27+	PCI Express Lane 27 Transmit +	DP-O	AC Coupled on Module	
D89	PCIE_TX27-	PCI Express Lane 27 Transmit -			
D90	GND	Power Ground	PWR GND		
D91	PCIE_TX28+	PCI Express Lane 28 Transmit +	DP-O	AC Coupled on Module	
D92	PCIE_TX28-	PCI Express Lane 28 Transmit -			
D93	GND	Power Ground	PWR GND		

Pin	COMe Signal	Description	Type	Termination	Comment
D94	PCIE_TX29+	PCI Express Lane 29 Transmit +	DP-O	AC Coupled on Module	
D95	PCIE_TX29-	PCI Express Lane 29 Transmit -			
D96	GND	Power Ground	PWR GND		
D97	RSVD	Reserved for future use	NC		
D98	PCIE_TX30+	PCI Express Lane 30 Transmit +	DP-O	AC Coupled on Module	
D99	PCIE_TX30-	PCI Express Lane 30 Transmit -			
D100	GND	Power Ground	PWR GND		
D101	PCIE_TX31+	PCI Express Lane 31 Transmit +	DP-O	AC Coupled on Module	
D102	PCIE_TX31-	PCI Express Lane 31 Transmit -			
D103	GND	Power Ground	PWR GND		
D104	VCC_12V	Main Input Voltage	PWR		
D105	VCC_12V				
D106	VCC_12V				
D107	VCC_12V				
D108	VCC_12V				
D109	VCC_12V				
D110	GND	Power Ground	PWR GND		

12/ uEFI BIOS

12.1. Starting the uEFI BIOS

Due to export control classification for the COMe-bDV7 the default BIOS has following features disabled:

- Intel AES-NI Encryption/Decryption
- Intel QuickAssist Technology

Contact your local Kontron sales or support for custom BIOS variants supporting the disabled features.

The COMe-bDV7 uses a Kontron-customized, pre-installed and configured version AMI UEFI BIOS Aptio ® V 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 COMe-bDV7.

The BIOS version covered in this document might not be the latest version. The latest version might have certain differences to the BIOS options and features described in this chapter.

Register for the EMD Customer Section to access BIOS downloads and the Product Change Notification (PCN) service.

The uEFI BIOS comes with a setup program that 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 board.
2. Wait until the first characters appear on the screen (POST messages or splash screen).
3. Press the <DEL> key.

If the uEFI BIOS is password-protected, a request for password will appear. Enter either the User Password or the Supervisor Password (see Chapter 12.2.4: Security Menu), press <RETURN>, and proceed with step 5.

4. A setup menu appears.

The COMe-bDV7 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 30: Navigation Hot Keys Available in the Legend Bar

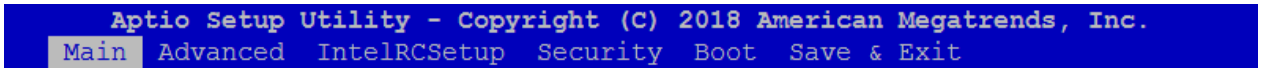
Sub-screen	Description
<F1>	<F1> key invokes the General Help window
<->	<Minus> key selects the next lower value within a field
<+>	<Plus> key selects the next higher value within a field
<F2>	<F2> key loads previous values
<F3>	<F3> key loads optimized defaults
<F4>	<F4> key Saves and Exits
<→> or <←>	<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

12.2. Setup Menus

The Setup utility features a selection bar at the top of the screen that lists the menus.

Figure 10: Setup Menu Selection Bar



The setup menus available for the COMe-bDV7 are:

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

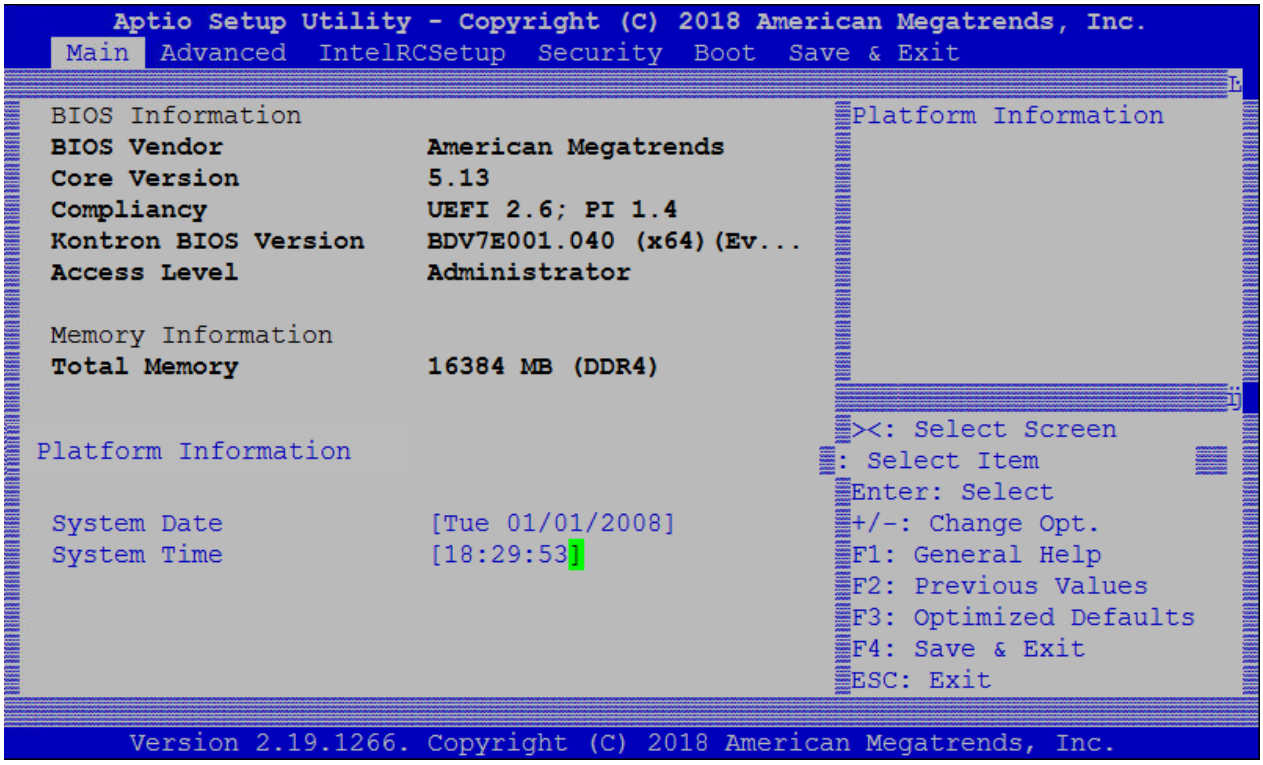
The currently active menu and the currently active uEFI BIOS setup item are highlighted in white. Use the left and right arrow keys to select the setup menus.

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.

12.2.1. Main Menu

On entering the uEFI BIOS, the setup program displays the Main setup menu that lists basic system information.

Figure 11: Main Setup Menu



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

Table 31: Main Setup Menu Functions

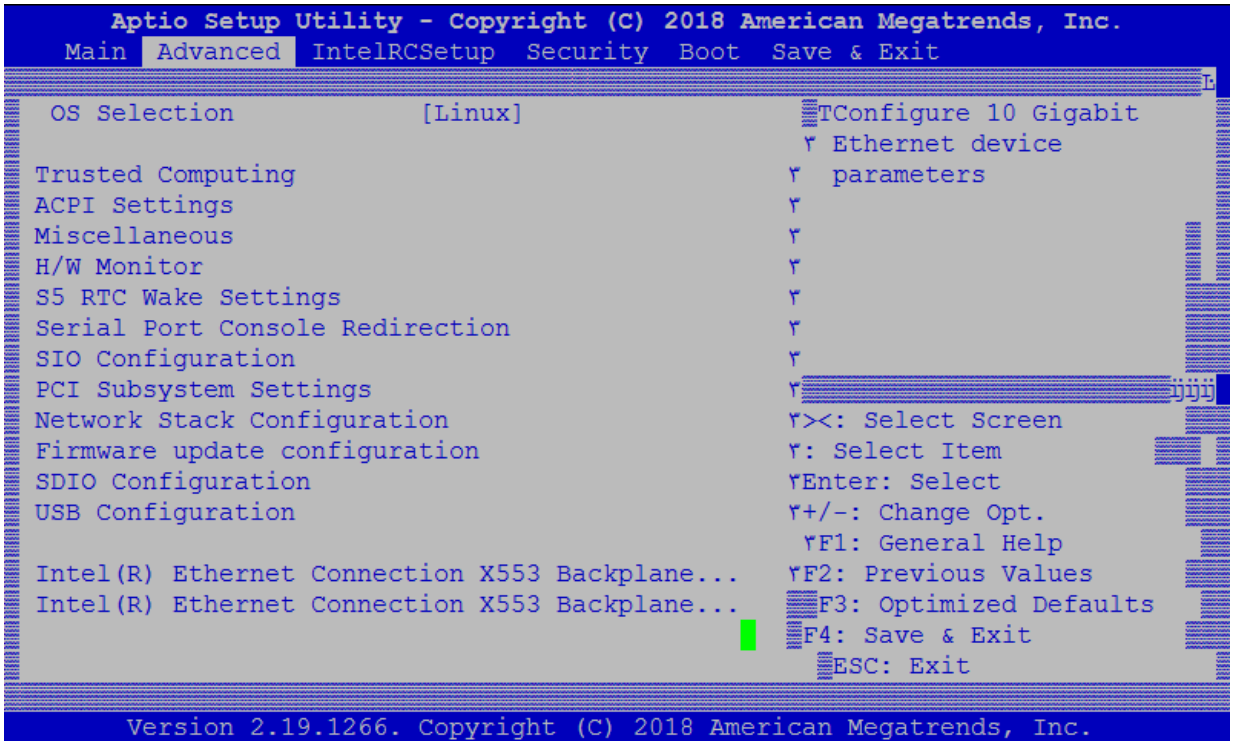
Sub-Screen	Description
BIOS Information	Read only field BIOS Vendor, Core Version, Compliancy, Kontron BIOS version, Access Level
Memory Information	Read only field Total memory
Platform Information	Read only field Include information about the platform such as Product Name, revision, Serial #, MAC Address, Boot Counter, CPLD Rev
System Date	Displays the system date [Week Day mm/dd/yyyy]
System Time	Displays the system time [hh:mm:ss]

12.2.2. Advanced Menu

The Advanced setup menu provides sub-screens and second level sub-screens with functions, for advanced configuration and Kontron specific configurations.

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

Figure 12: Advanced Setup Menu



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

Table 32: Advanced Setup Menu Functions

Sub-Screen	Second Level Sub-screen	Further Sub-Screens/Description
OS selection	Selects the OS as the uARTS need different IROs for Windows and Linux [Windows, **Linux**]	
Trusted Computing	BIOS support for security device. Operating System will not show security device. The TCG EFI protocol and INT1A interface are not available. [Enabled, **Disabled**]	
ACPI Settings	Enable ACPI Auto Conf.	ACPI auto configuration [Enabled, **Disabled**]
	Enable Hibernation	System's ability to hibernate (OS/S4 Sleep State) Note : This option may not be effective with some operating systems. [**Enabled**, Disabled]
	Lock Legacy Resources	Lock of legacy resources [Enabled, **Disabled**]

Sub-Screen	Second Level Sub-screen	Further Sub-Screens/Description	
Miscellaneous	Watchdog	Auto Reload	Automatic reload of watchdog timers on timeout [Enabled, **Disabled**]
		Global Lock	Enable sets all Watchdog registers (except for WD_KICK) to read only, until board is reset. [Enabled, **Disabled**]
		Stage 1 Mode	Selects action for this Watchdog stage [**Disabled**, Reset, NMI, SCI, Delay, WDT Signal only]
	Reset Button Behavior	Selects reset button behavior [**Chipset Reset**, Power Cycle]	
	I2C Speed	Selects I2C bus speed (Range- 1 kHz to 400 kHz) Default - 200KHz . [**200**]	
	Onboard I2C Mode	[**Multimaster**, Busclear]	
	Manufacturing Mode	Read only field [**Disabled**]	
	LID Switch Mode	Shows or hides Lid Switch Inside ACPI OS. [**Disabled,** Active-normal, Active-inverse]	
	Sleep Button Mode	Shows or hides Sleep Button inside ACPI OS. [Enabled, **Disabled**]	
	ACPI Temperature Poll	Sets temperature polling mode through OSPM (0 =disabled, 1= enabled) [**Enabled,** Disabled]	
	TZ00 Temperature Poll	Interval (sec.) between two temperature measuring attempts in ACPI thermal zone 00 (Ambient Temperature) [**30**]	
	TZ01 Temperature poll	Interval (sec.) between two temperature measuring attempts in ACPI thermal zone 01 (CPU Temperature) [**30**]	
	SMBus Device ACPI Mode	Hides SMBus device from OS, otherwise the device is visible in OS. [**Normal**, Hidden]	
	CPLD Device ACPI Mode	Hides CPLD device from OS, otherwise the device is visible in OS. [**Normal**, Hidden]	
H/W Monitor	Read only fields Hardware Monitor Name: CPU temperature: Module temperature:		
	CPU Fan - showing current RPM		
	Fan Control	Sets CPU fan control mode. Note: Disable - stops fan [Disable, Manual, **Auto**]	
	Fan Pulse	Pulses fan produces during 1 revolution. (Range: 1-4) [**2**]	
	Fan Trip Point	Temperature at which the fan accelerates. (Range: 20°C – 80°) [**50**]	
	Trip Point Speed	Fan speed at trip point in %. Min. value is 30 %. Fan always runs at 100 % at TJmax - 10°C. [**50**]	

Sub-Screen	Second Level Sub-screen	Further Sub-Screens/Description	
H/W Monitor (continued)	Ref. Temperature	Temperature source for automatic fan control [PCH Temperature, Module Temperature, **CPU Temperature**]	
	External Fan – showing current RPM		
	Fan Control	Sets fan control mode Note: Disable - stops fan [Disable, Manual, **Auto**]	
	Fan Pulse	Pulse fan produces during 1 revolution (Range: 1-4) [**2**]	
	Fan Trip point	Temperature at which fan accelerates. (Range: 20°C to 80°C) [**50**]	
	Trip Point Speed	Fan speed at trip point in %. Minimum value is 30% Fan always runs at 100% at TJmax (-10°C) [**50**]	
	Read only field 5.0V Standby: Batt Volt. at COMe Pin: Widerange VCC:		
S5 RTC Wake Settings	System wake on alarm event. [**Disables**, Fixed Time, Dynamic Time]		
Serial Port Console Redirection	COM0		
	Console Redirection	[**Enabled**, Disabled]	
	Console Redirection settings	Specify how the host computer and remote computer exchange data. Both computers should have the same settings.	
		Terminal Type	[**ANSI]**
		Bits per second	[**115200**]
		Data Bits	[**8**]
		Parity	[**None**]
		Stop Bits	[**8**]
		Flow Control	[**None**]
		VT-UTF8 Combo Key Sup	[**Enabled**]
		Recorder Mode	[**Disabled**]
		Resolution 100x31	[**Disabled**]
		Putty keyPad	[**VT100**]
	COM1		
	Console Redirection	[Enabled, **Disabled**]	
	Serial Port for Out-of-Band Management / Windows EMS		
	Console Redirection	[**Enabled**, Disabled]	
	Console Redirection Settings	Microsoft Windows Emergency Management Services (EMS)allows remote management of a Windows Server OS through a serial port	
		Terminal Type	[**VT-UTF8**]
		Bits per second	[**115200**]
		Flow control	[None]

Sub-Screen	Second Level Sub-screen	Further Sub-Screens/Description	
Serial Port Console Redirection (continued)	Console Redirection Settings (continued)	Read only fields Date Bits Parity Stop Bits	
SIO Configuration	Read only field AMI SIO Driver Version		
	Super IO Chip Logical Device(s) Configuration		
	Serial Port 1	Use This Device	Enable or disable this logical device. [**Enabled**, Disabled]
		Logical Device Settings	
		Current	Read only field To refresh- reset required
		Possible	Changes device's resource settings. New settings are reflected on the setup page after system restarts. [**Use Automatic Settings**]
	Read Only field Warning: Disabling SIO logical devices may have unwanted side effects. PROCEED with CAUTION.		
	Serial Port 2	Use This Device	Enable or disable this logical device. [**Enabled**, Disabled]
		Logical Device Settings	
		Current	Read only field To refresh- reset required
		Possible	Change device's resource settings. New settings are reflected on the setup page after system restarts. [**Use Automatic Settings**]
	Read only field Warning: Disabling SIO logical devices may have unwanted side effects. PROCEED with CAUTION.		
	Parallel Port	Use This Device	Enable or disable this logical device. [**Enabled**, Disabled]
		Logical Device Settings	
		Current	Read only field To refresh- reset required
		Possible	Change device's resource settings. New settings are reflected on the setup page after system restarts. [**Use Automatic Settings**]
	Read only field Warning: Disabling SIO logical devices may have unwanted side effects. PROCEED with CAUTION.		
	PS2 Controller (KB&MS)	Use This Device	Enable or disable this logical device. [**Enabled**, Disabled]
		Logical Device Settings:	
		Current	Read only field To refresh- reset required

Sub-Screen	Second Level Sub-screen	Further Sub-Screens/Description	
SIO Configuration (continued)	PS2 Controller (KB&MS) (continued)	Possible	Change device's resource settings. New settings are reflected on the setup page after system restarts. [**Use Automatic Settings**]
	Read only field Warning: Disabling SIO logical devices may have unwanted side effects. PROCEED with CAUTION.		
	Floppy disk Controller Configuration	Use This Device	Enable or disable this logical device. [**Enabled**, Disabled]
		Logical Device Settings:	
		Current	Read only field To refresh- reset required
		Possible	Change device's resource settings. New settings are reflected on the setup page after system restarts. [**Use Automatic Settings**]
	Read only field Warning: Disabling SIO logical devices may have unwanted side effects. PROCEED with CAUTION		
PCI Subsystem Settings	Read only field PCI Bus Driver version		
	PCI Device Common settings:		
	PCI –Latency Timer	Number PCI bus clocks programmed in PCI latency timer register [**32**, 64, 96, 128, 160, 192, 224, 248]	
	PCI-X Latency Timer	Number PCI bus clocks programmed in PCI X latency timer register [32, **64**, 96, 128, 160, 192, 224, 248]	
	VGA Palette Snoop	[Enabled, **Disabled]**	
	PERR# Generation	[Enabled, **Disabled**]	
	SERR# Generation	[Enabled, **Disabled**]	
	Above 4G Decoding	64-bit capable devices to be decoded in the above 4G address space. Note: Only if system supports 64-bit PCI decoding. [Enabled, **Disabled**]	
	SR-IOV Support	Single Root IO virtualization support If PCIe devices are SR-IOV capable. [**Enabled**, Disabled]	
	BME DMA Mitigation	Re-enable Bus master attribute disabled during PCI enumeration for PCI Bridges after SMM lock [Enabled, **Disabled**]	
	PCI Express Settings	PCI Device register Settings	
		Relaxed Ordering	[Enabled, **Disabled**]
		Extended Tag	If enabled can use 8-bit Tag field as a requester. [Enabled, **Disabled**]
		No Snoop	[**Enabled**, Disabled]
		Maximum Payload	Sets max. payload of PCIe device or allows system BIOS to select automatically.

Sub-Screen	Second Level Sub-screen	Further Sub-Screens/Description	
PCI Subsystem Settings (continued)	PCI Express Settings Continued)	Maximum Payload (continued)	[**Auto**, 128 Bytes, 256 Bytes, 512 bytes, 1024 bytes, 2048 Bytes, 4096 Bytes]
		Maximum Read Request	Sets Max. read request size of PCI Express device or allows system BIOS to select.. [**Auto**, 128 Bytes, 256 Bytes, 512 bytes, 1024 bytes, 2048 Bytes, 4096 Bytes]]
		PCI Express Link Register Settings	
		ASPM Support	Sets ASPM level, where Auto selects BIOS auto conf. [Auto, **Disabled**]
		Warning Enabling ASPM may cause some PCI-E devices to fail.	
		Extended Synch	Allows Extended synchronization patterns. [Enabled, **Disabled**]
		Link Training Retry	Number of retry attempts to retain link if a previous training attempt was unsuccessful [Disables, 2, 3, **5**]
		Link Training Timeout	Number of msec software waits before polling link training bit in Link status register. Range (10-10000 µs) [**1000**]
		Unpopulated Links	Setting disable link disables unpopulated PCI express links to save power [**Keep Link On**, Disable Link]
	PCI Express GEN 2 Settings	PCI Express Gen2 Device Register Settings	
		Completion Timeout	Modifies completion timeout value. Range 50µs-50ms. [**Default**, Shorter, Longer, Disabled]
		ARI Forwarding	If supported by hardware and set to enabled, the downstream port disables its traditional device number field being 0 enforcement when turning a Type 1 Configuration request into a Type0 Configuration request, permitting access to Extended Functions in an ARI Device immediately below the port. Default value is disabled. [Enabled, **Disabled**]
		Atomic Op Requester Enable	Initiates AtomicOP requests only if bus master enable bit is set in the Command Register Set. [Enabled, **Disabled**]
		AtomicOP Egress Block	Outbound AtomicOp requests via Egress ports are blocked. [Enabled, **Disabled**]
		IDO request Enable	Permits setting number of ID-based ordering (IDO) bit (attribute [2]) requests to be initiated. [Enabled, **Disabled**]
		IDO Completion Enable	Permits setting number of ID-based ordering (IDO) bit (attribute [2]) requests to be initiated. [Enabled, **Disabled**]

Sub-Screen	Second Level Sub-screen	Further Sub-Screens/Description	
PCI Subsystem Settings (continued)	PCI Express GEN 2 Settings (continued)	LTR Mechanism Enable	Enables latency tolerance reporting (LTR) [Enabled, **Disabled**]
		End-End TLP Prefix B1	Blocks forwarding of TLPs containing End-End TLP prefixes. [Enabled, **Disabled**]
		PCI Express GEN2 Link Register Settings	
		Target Link Speed	Sets the upper limit on link operational speed If set to Force to X.X GT/S for downstream ports. [**Auto**, Force to 2.5GT/s, Force to 5GT/s, Force to 8GT/s]
		Clock Power Management	Permitted to use CLKREQ# signal for power management of link clock in accordance to protocol. [Enabled, **Disabled**]
		Compliance SOS	Forces LTSSM to send SKP ordered sets between sequences when sending Compliance Pattern or Modified Compliance. [Enabled, **Disabled**]
		Hardware Autonomous Width	Disables hardware's ability to change link width (except width size reduction for correction purposes). [**Enabled**, Disabled]
		Hardware Autonomous Speed	Disables hardware's ability to change link speed (except speed rate reduction for correction purposes). [**Enabled**, Disabled]
Network Stack Configuration	UEFI network stack. [Enabled, **Disabled**]		
Firmware Update Configuration	Allows BIOS re-flashing as far as relax security configuration is set to enable. [Enabled, **Disabled**]		
SDIO	Read only field List the Mass Storage Devices and supplies BUS, DEV abd FUNc information		
	SDIO Access Mode	For the listed mass storage device the options are and set the mode to access the SD device. Note : Auto – accesses SD device in DMA mode, if controller supports, this mode otherwise in PIO mode. [**Auto**, ADMA , SDMA, PIO]	
	MMC device	Mass storage device demulation type. Auto numerates devices less than 530 MB as floppies. Force FDD can be used to force HDD formatted drive to boot as FDD. [Auto, Floppy , Forced FDD, Hard Disk]	
USB Configuration	Read only fields UBS Module Version, USB Controllers USB devices		
	Legacy USB Support	Auto disables legacy support, if no USB devices are connected and Disable keeps USB devices available for EFI applications only. [**Enabled**, Disabled, Auto]	

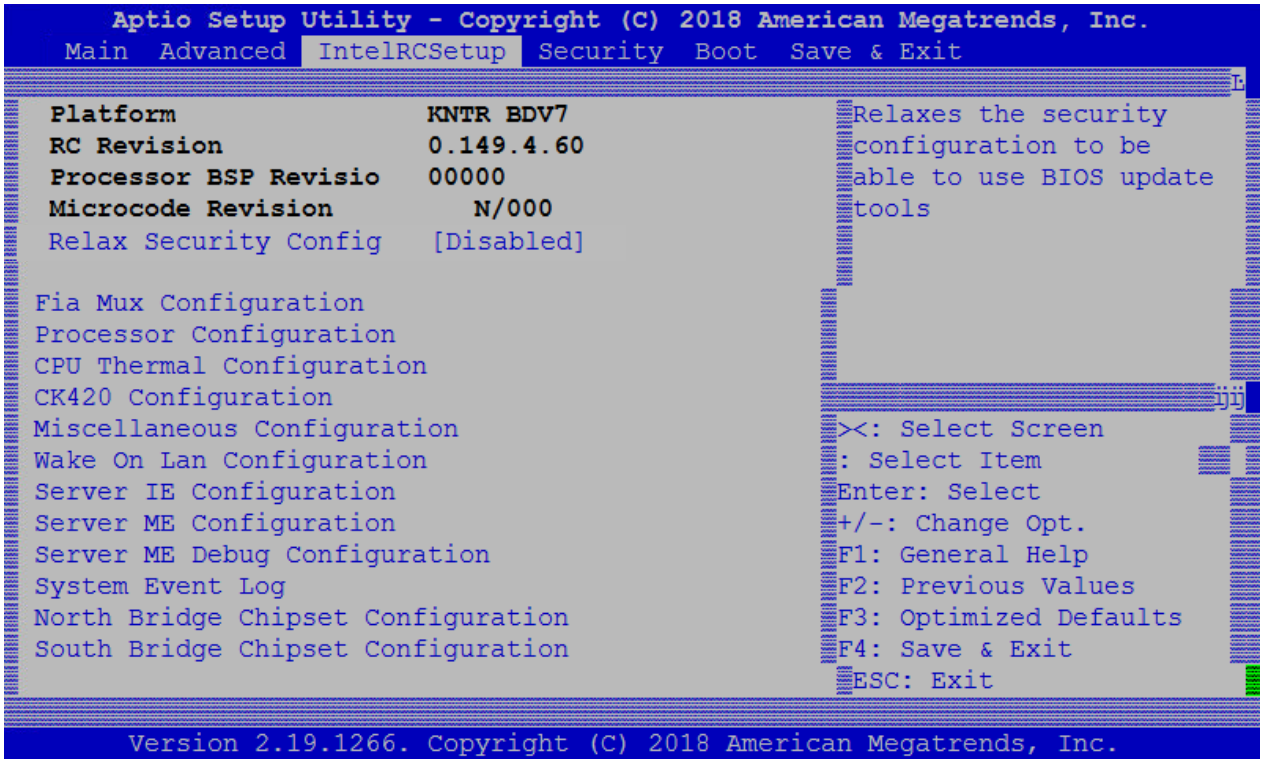
Sub-Screen	Second Level Sub-screen	Further Sub-Screens/Description	
USB Configuration (continued)	XHCI Hand-off	XHCI ownership change should be claimed by XHCI driver. Note: this is a work around for OS(s) without XHCI hand-off support. [**Enabled**, Disabled]	
	USB Mass Storage Driver Support	[**Enabled**, Disabled]	
	Port 60/64 Emulation	I/O port 60h/64h emulation support Note: Enable for USB keyboard legacy support for non-USB aware OS(s). [**Enabled**, Disabled]	
	USB Hardware delays		
	USB Transfer Time-out	Timeout value of control, bulk and interrupt transfers [**20 sec**]	
	Device Reset Time-out	Timeout value of USB mass storage device start unit command time-out [**20 sec**]	
	Device Power-up Delay	Max. time for device to report to host controller. Auto uses root port default value 100 ms, for hub port delay is taken. [**Auto,** Manual]	
Intel® Ethernet Connection X553 Backplane	NIC Configuration	Wake On LAN	Enables system power-on via LAN. Note that configuring Wake on LAN in OS does not change value of this setting but overrides the behavior. [**Enabled**, Disabled]
		Link Speed	Read only field [**Auto Negotiated**]
	Blink LED	Identify the physical Network port by blinking the associated LED [**0**]	
	Read only field UEFI Driver, Adapter PBA, Device Name, Chip Type, PCI Device ID, PCI Address, Link status, MAC Address, Virtual MAC Address		
Intel® Ethernet Connection X553 Backplane	NIC Configuration	Wake On LAN	Enables system power-on via LAN. Note that configuring Wake on LAN in OS does not change value of this setting but overrides the behavior. [**Enabled**, Disabled]
		Link Speed	Read only field [**Auto Negotiated**]
	Blink LED	Identify the physical Network port by blinking the associated LED [**0**]	
	Read only field UEFI Driver, Adapter PBA, Device Name, Chip Type, PCI Device ID, PCI Address, Link status, MAC Address, Virtual MAC Address		
Intel® Ethernet Connection X553 Backplane	NIC Configuration	Wake On LAN	Enables system power-on via LAN. Note that configuring Wake on LAN in OS does not change value of this setting but overridse the behavior. [**Enabled**, Disabled]
		Link Speed	Read only field [**Auto Negotiated**]
	Blink LED	Identify the physical Network port by blinking the associated LED [**0**]	
	Read only field UEFI Driver, Adapter PBA, Device Name, Chip Type, PCI Device ID, PCI Address, Link status, MAC Address, Virtual MAC Address		

Sub-Screen	Second Level Sub-screen	Further Sub-Screens/Description	
Intel® Ethernet Connection X553 Backplane	NIC Configuration	Wake On LAN	Enables system power-on via LAN. Note that configuring Wake on LAN in OS does not change value of this setting but overrides the behavior. [**Enabled**, Disabled]
		Link Speed	Read only field [**Auto Negotiated**]
	Blink LED	Identify the physical Network port by blinking the associated LED [**0**]	
	Read only field UEFI Driver, Adapter PBA, Device Name, Chip Type, PCI Device ID, PCI Address, Link status, MAC Address, Virtual MAC Address		

12.2.3. InterlRCSetup Menu

The IntelRCsetupSetup menu provides sub-screens and second level sub-screens for processor related functions.

Figure 13: IntelRCSetup



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

Table 33: InterlRCSetup Setup Menu Functions

Function	Second level Sub-Screen / Description	
Read Only field Platform, RC Revision, Processor BSP Revision and Microcode revision		
Relax security Configuration	Relaxes security configuration to be able to use BIOS update tools [Enabled, **Disabled**]	
Fia Mux Configuration	By enabling this function users can override the platform configuration on FIA/WM	
	Bifurcation Control 0	Selects the type of Bifurcation [**P3P2P1P0 X2X2X2X2,** **P3P2—P0 X2X2X4** **--P2P1P0 X4X2X2** **--P2—P0 X4X4** **------P0 X8**]
	Bifurcation Control 1	
	Lane [0 to 19]	Lanes can be set to PCIE, XHCI , SATA or Lane Disabled [**lane Disabled**]

Function	Second level Sub-Screen / Description	
Fia Mux Configuration (continued)	**Additional Information:** The HSIO lanes [0-19] support the following: Lanes [0-3] -Lane Disabled or PCIE Function Lanes [4-15] - Lane Disabled, PCIE Function or SATA Function Lanes [16-19] - Lane Disabled, SATA Function or XHCI Function	
	PCIE Root Port Link Width Control	
	Root port [0 to 7] Link Width	BICTRL keeps Bifurcation setting and X1 forces width 1 [**BICTRL, X1**]
Processor Configuration	Read only field Processor ID, Processor frequency, CPU BCLK frequency, L1 cache and L2 Cache RAM, Processor version	
	EIST (GV3)	GV3 and TM1 must be enabled for TM2 to be available and GV3 must be enabled for Turbo. Auto enable for B0 CPU stepping, all others disabled, change settings to override. [**Enabled**, Disabled]
	BIOS Request Frequency	Two modes min. and max. frequency, CPU instructed to provide highest possible legal frequency to the processor [**Enabled**, Disabled]
	Turbo	For CPU turbo capability. This option on applies to ES2 and above. [**Enabled**, Disabled]
	TM1	Note: TM1 And GV3 must be enabled in order to support TM2. [**Enabled**, Disabled]
	TM2 Mode	LFM throtting or adaptive throttling for TM2 mechanisms. [LFM throttling, **Adaptive Throttling**]
	Dynamic Self refresh	Dynamic self refresh in memory controller. [Enabled, **Disabled**]
	PMOP levels	Power Mode OP code (PMOP) speed during self refresh [slow, **Fast**]
	CPU c state	Enhances CPU Cx state, takes effect after reboot. [**Enabled**, Disabled]
	Package C-State Limit	[No Pkg C-state, No SOIx, **No limit**]
	Max. Core C-State	[C1, **C6**]
	Enhanced Halt State	Enhances CPU C1E state takes effect after reboot. [**Enabled**, Disabled]
	Monitor/MWait	[**Enabled**, Disabled]
	L1 Prefetcher	[**Enabled**, Disabled]
	L2 Prefetcher	[**Enabled**, Disabled]
	ACPI 3.0 T-States	[Enabled, **Disabled**]
	Fast String	Enables fast string for REP MOVS/STOS [**Enabled**, Disabled]
	Machine Check	[**Enabled**, Disabled]

Function	Second level Sub-Screen / Description		
Processor Configuration (continued)	Max COUID Value Limit	Enable to boot legacy OSs that cannot support CPUs with extended CPUID functions [Enabled, **Disabled**]	
	Execute Disable Bit	Disable forces XD flag to always return (0) [**Enabled**, Disabled]	
	VMX	Vanderpool Technology, takes effect after reboot [**Enabled**, Disabled]	
	BIST Selection	[Enabled, **Disabled**]	
	Extened APIC	Read only field [**Enabled**, Disabled]	
	MSR 606 PKG_Power_SKU	Read only field [**330a0e08**]	
	Active processor Core	Number of active Processor Cores in SoC. (where 0 = all existing processor cores active) [**0**]	
	Dump Crash Log	[Enabled, **Disabled**]	
	CPU Flex Ratio Override	[Enabled, **Disabled**]	
	CPU Core Ratio	Read only field [**24**]	
	Ratio Limits Configuration	Configuration of Ratio Limits MSRs [Enabled, **Disabled**]	
CPU Thermal Configuration	TJ target	Offset below TJmax set as PROCHOT# activation temp Range 0°C to 63°C [**0**]	
	Tcontrol Offset	Offset to modify TControl for DTS2.0, Range 0°C to 63°C [**0**]	
	Tcontrol Offset Sign	Sign for the Tcontrol Offset value [**Positive,** Negative]	
	TM1	Note: TM1 and GV3 must be enabled in order to support TM2 [**Enabled**, Disabled]	
	TM2 Status	Read only field [**Enabled**]	
	TM2 Mode	Selects LFM throtting or adaptive throttling for TM2 mechanisms. [LFM throttling, **Adaptive Throttling**]	
	CPU DFX Thermal Configuration	Out of Spec Interrupt	Generates thermal interrupt, whenever out of spec. temperature threshold crossed [Enabled, **Disabled**]
		Low Temperature Interrupt	Triggers input when temperature goes from HOT to NOT_HOT [Enabled, **Disabled**]
		High Temp Interrupt	Triggers input when temperature goes from NOT_HOT to HOT [Enabled, **Disabled**]

Function	Second level Sub-Screen / Description		
CPU Thermal Configuration (continued)	CPU DFX Thermal Configuration (continued)	Threshold 1 Rel Temp	Degrees below TJMax to signal an interrupt whenever temperature crosses this threshold. (Range 0°C – 127°C) [**5**]
		Threshold 2 Rel temp	Degrees below TJMax to signal an interrupt whenever temperature crosses this threshold. (Range 0°C – 127°C) [**10**]
		Threshold 1 Interrupt	Generates thermal Interrupt whenever Threshold 1 crossed. [Enabled, **Disabled**]
		Threshold 2 Interrupt	Generates thermal Interrupt whenever Threshold 2 crossed. [Enabled, **Disabled**]
		External PROCHOT Interrupt	Generates Interrupt when an external device drives the PROCHOT# pin. [**Enabled**, Disabled]
		PROCHOT Response	Internal Intel Only: UCode will copy this value to/from PCU_CR_Firm_Config(12). [Enabled, **Disabled**]
		PROCHOT Output Mode Disable	Internal Intel Only: Prochot output disable UCode will copy this value to/from PCU_CR_Firm_Config(11). [**Enabled**, Disabled]
		VR_Therm_Alert_ Disable	1= disable VR_Thermal_Alert signaling. Internal Intel Only: Disable SVID during bclk overclocking mode. This bit of mirror of PCU_CR_Firm_Config(14). [Enabled, **Disabled**]
		Prochot frequency Res…..	Controls the level of PROCHOT throttling. [Enabled, **Disabled**]
		Lock_Therm_INT	Ties thermal interrupts from both cores (thermal interrupt on one core routed to all cores) [Enabled, **Disabled**]
CK420 Configuration	Spread Spectrum OFF/ON [**Enabled**, Disabled]		
Miscellaneous Configuration	Core-Uncore BGF Point	BGF pointer separation [8, **4**, 2]	
	Active SATA Boot Device	[**Onboard device**, PCIE device]	
	Inspectrum	Required to test PCIe CLB [Enabled, **Disabled**]	
	Enable Modphy for I/O Compliance	[SATA DTLE=7, SATA3 DTLE=3, **Disabled**]	

Function	Second level Sub-Screen / Description		
Wake on LAN	Wake on LAN Configuration setting [**Enabled**, Disabled]		
Server IE Configuration	Read only Field IE Firmware Status #1, IE Firmware Status #2		
	HECI-1 Enable	Override HECI-1 Status on PCI [Enabled, **Disabled**]	
	HECI-2 Enable	Override HECI-2 Status on PCI [Enabled, **Disabled**]	
	HECI-3 Enable	Override HECI-3 Status on PCI [Enabled, **Disabled**]	
	IDER Enable	Override IDER Status on PCI [Enabled, **Disabled**]	
	KT Enable	Override KTStatus on PCI [Enabled, **Disabled**]	
	Subsystem ID	Subsystem ID of IE devices **8086**	
Server ME Configuration	Read Only Field Operational Firmware ME firmware type Backup firmware version Recovery firmware version, ME firmware features, ME firmware status #1 ME Formware status #2 Current state Error code		
	MCTP Bus Owner	MCTP bus owner location on PCIe: [15:8] bus, [7:3] device, [2:0] function. If all zero sending bus owner is disabled. [**0**]	
	ME shutdown message	Sends ME_shutdown message to ME when launching OS [Enabled, **Disabled**]	
	ICC Clock SSC	Overridse SSC setting for ICC clock, or lets firmware decide based on platform type- [Enabled, Disabled, **Auto**]	
Server ME debug Configuration	NM Configuration	ME Initialization Complete Timeout	How long BIOS waits for ME to initialize. [**2**]
		Enable HSIO Messaging	[**Enabled**, Disabled]
		Enable FIA MUX Messaging	[**Enabled**, Disabled]
		DRAM Init Done Enable	Notifies ME about DRAM initializion. (enables/ disables UMA functionality) [**Enabled**, Disabled]

Function	Second level Sub-Screen / Description		
Server ME debug Configuration (continued)	NM Configuration (continued)	DRAM Init Done Time	Waiting for DRAM initialization notify acknowledge from ME with 5 sec timeout [**Enabled**, Disabled]
		DRAM Initialization	Overrides DRAM Initialization [Auto- true status, 0- success, 1- No memory in channels, 2- Memory Init Error]
		HMRFPO_lock_ enable	Sends HMRFPO_lock message to ME [**Enabled**, Disabled]
		HMRFPO_ENABLE Message	Sends HMRFPO_Enable message to ME [Enabled, **Disabled**]
		End_of_Post Message	Sends End_of_post message to ME [**Enabled**, Disabled]
		CG9 global reset prom	Prompta CF9 reset to global [Enabled, Disabled]
		Global reset lock	Locks the joint ME and host reset capability [**Enabled**, Disabled]
		HECI-1 Enable	Override HECI-1 status on PCI, or let firmware decide based on ME type (Auto) [Enabled, Disabled, **Auto**]
		HECI-2 Enable	Override HECI-2 status on PCI, or let firmware decide based on ME type (Auto) [Enabled, Disabled, **Auto**]
		HECI-3 Enable	Override HECI-3 status on PCI, or let firmware decide based on ME type (Auto) [Enabled, Disabled, **Auto**]
		IDEr Enable	Override IDErstatus on PCI, or let firmware decide based on ME type (Auto) [Enabled, Disabled, **Auto**]
		KT Enable	Override IKTon PCI, or let firmware decide based on ME type (Auto) [Enabled, Disabled, **Auto**]
		HECI-1 Hide in ME	Enables sending request to ME to hide or disable HECI-1 on host PCI [**Off**, Hide, Disable]
		HECI-2 Hide in ME	Enables sending request to ME to hide or disable HECI-2 on host PCI [**Off**, Hide, Disable]
System Event Log	System Errors	Auto = enabling/disabling of errors in the driver is skipped. [**Enabled**, Disabled, Auto]	
	Memory Event log	Memory Elog Support	[Enabled, Disabled]
		Parity Check	[Enabled, Disabled]

Function	Second level Sub-Screen / Description		
System Event Log (continued)	Memory Event log (continued)	Log Correctable Error	[Enabled, Disabled]
		Log Un-correctable Error	[**Enabled**, Disabled]
		Enable /Disable Error	Error clocking feature to hide CE errors to OS [Enabled, **Disabled**]
	PCIe Event Log	PCIe ELog Support	[**Enabled**, Disabled]
		Log Fatal Error	Sends system event signal on fatal error [**Enabled**, Disabled]
		LOG Non-Fatal Error	Sends system event signal on non-fatal error [**Enabled**, Disabled]
		Log correctable Error	Sends system event signal on correctable error [**Enabled**, Disabled]
		PCIe System Error	System error reporting on all enumerated root ports, bridges and devices [**Enabled**, Disabled]
		PCIe Parity Error	Parity error reporting on all enumerated root ports, bridges and devices [**Enabled**, Disabled]
	Whea Settings	WHEA support	[**Enabled**, Disabled]
		WHEA Error Injection	WHEA EINJ ACPI 5.0 support for set error types with address and vendor extensions [**Enabled**, Disabled]
		WHEA logging	WHEA logging of errors [**Enabled**, Disabled]
		WHEA PCIE Error Injection	WHEA PCIE Error Injection [**Enabled**, Disabled]
North Bridge Chipset Configuration	Read only field Memory information: MRC version, Total memory, Memory frequency		
	Pass Gate Setup	Mitigation Feature Configuration:	
		Mitigation Feature Enable	[Enabled, **Disabled**]
		Pass Gate Stress Test Configuration:	
		Pass Gate Test	[Enabled, **Disabled**]
		Pass Gate test Direction	[**lowest->highest,** highest->lowest]
		Pass Gate Test Repetition	Count range over same row **900**
		Pass Gate Test Iteration	Iterations on row **1**

Function	Second level Sub-Screen / Description		
North Bridge Chipset Configuration (continued)	Pass Gate Setup (continued)	Pass Gate Test Swizzle	Forces Sizzle mode (Samsung) [**Auto,** Enabled]
		Pass Gate Test pattern	[**0's**]
		Pass Gate Test Target Pattern	[**1's**]
		Pass Gate Test speed	Speed of characterization test [1x only, 2x only, 4x only,**8x only**]
		Pass Gate Partial	[Enabled, **Disabled**]
		Row Bank Min.	Minimum address to test depending on DDR3 /DDR4 **...0**
		Row Bank Max.	Minimum address to test depending on DDR3 /DDR4 **....8**
		Channel 0:	
		Rank 0	[**Enabled**, Disabled]
		Rank 1	[**Enabled**, Disabled]
		Channel 1	
		Rank 0	[**Enabled**, Disabled]
		Rank 1	[**Enabled**, Disabled]
		Pass Gate MonteCarlo	Search algorithm to find PG max. [**Disabled**]
		Pass Gate Max. Failure	Read only field 500
		Pass Gate MonteCarlo	Read only field 900
		Pass Gate MonteCarlo	Read only field 10
	Leaky Bucket Setup	Channel 0:	
		Leak Rate Configuration	[**Days,** microseconds]
		Rank 0	0
		Rank 1	0
		Channel 1:	
		Rank 0	0
		Rank 1	0
		Correctable Error Threshold	
		Rank 0	0
		Rank 1	0
		Channel 1:	

Function	Second level Sub-Screen / Description		
North Bridge Chipset Configuration (continued)	Leaky Bucket Setup (continued)	Rank 0	0
		Rank 1	0
	Non Volatile memory Setup	Read only data SoC Pwr los support, cashe Flushinh, ADR State Source, Internal Pwr Loss Event Setup, Interleaving, restore, Erase and Arm, NVDIMM Battery, LBA start location, LBA, Size (8MB), Test Non-Vol Mode	
	Fast Boot	Skips memory training and attempts to boot using last known good configuration [Enabled, **Disabled**]	
	Command Mode	[1N, **2N**]	
	Smm size (MB)	Size of SMM/TSEG region in (MB) [2, 4, 8, **16**]	
	Command Address Parity	[Enabled, **Disabled**]	
	Memory Frequency	[DDR-1600, DDR-1877, DDR-2133, **DDR-2400**]	
	Enable 32-bit Bus	[Enabled, **Disabled**]	
	TCL Performance	[**Enabled,** Disabled]	
	Enable Parallel Train	Algorithm runs in parallel [Enabled, **Disabled**]	
	Memory Channels	[**Dual Channel,** Single Channel]	
	MRC Debug Message	Displays debug output in MRC [Disabled, Minimum, **Medium,** Maximum, General options]	
	Memory Preservation	Memory content preservation. with warm reset [**Enabled,** Disabled]	
	Fine Ddr Voltage	Range –100 mV to 100 mV in 5 mV steps **100**	
	Read per bit Training	[**Enabled,** Disabled]	
	Write per bit Training	[**Enabled,** Disabled]	
	EEC Support	[**Enabled,** Disabled]	
	Faulty Part Tracking	[Enabled, **Disabled**]	
	On Correctable faulty	Read only field [**Halt**]	
	Patrol Scrub Enable	[**Enabled,** Disabled]	
	Patrol Scrub Period	[**24 hours**, 10 hours, 4 hours, 1 hour]	
	Demand Scrub Enable	[**Enabled,** Disabled]	
	AB Segments in DRAM	Reads & write targeting segment A or B routed to DRAM [Enabled, **Disabled**]	

Function	Second level Sub-Screen / Description	
North Bridge Chipset Configuration (continued)	E Segments in DRAM	Reads & write targeting segment E routed to DRAM [**Enabled,** Disabled]
	F Segments in DRAM	Reads & write targeting segment F routed to DRAM [**Enabled,** Disabled]
	ZQ Calibration	[**Enabled,** Disabled]
	Rank Margin Tool	[Enabled, **Disabled**]
	RMT CPGC Exp_loop_cnt	Set for field for RMT execution [1,2,3,4,5,6,7,8,9,10,11,**12**]
	RMT CPGC Num_bursts	Sets field for RMT execution [1,2,3,4,5,**6**,7,8,9,10,1,12]
	Out of order Memory Processing	[**Enabled,** Disabled]
	Read two Clocks Preamble	[Enabled, **Disabled**]
	Write two Clocks Preamble	[Enabled, **Disabled**]
	Write Data Early Enable	[Enabled, **Disabled**]
	Out of Order Aging threshold	8
	New Request Bypass	New request skip queue and are processed immediately if queue empty [**Enabled,** Disabled]
	Select Refresh Rate	[1x/2x/4x, **x1/x2**]
	CKE Power Down	[Active Power down, Precharge power down, **Disabled**]
	RAPL Time window	DDRAM RAPL time window for PL1 **0**
	RAPL Power limit Enable	[Enabled, **Disabled**]
	RAPL Power limit	DDRAM RAPL power limit[1] for DDR Domain (mW) **2047875**
	Lock MSR 618 DDR_RAPL	[**Enabled**, Disabled]
	PMOP Value for PC0	Power mode OPcode for PC0 **4**
	PMOP Value for PCX	Power mode OPcode for PC0 **7**
	Open Page Policy Time	[**Disabled,** Immediate, 30-60 ns, 60-120 ns, 120-240 ns, 240-480 ns, 480- 960 ns, 1-2 µs]
	Memory Thermal Throttle	[**Auto,** Disabled]
	Thermal Throttling	[**CLTT**, OLTT]
	CLTT Mode	[**Normal,** Pass thru]

Function	Second level Sub-Screen / Description		
North Bridge Chipset Configuration (continued)	High Temperature	Temperature in°C.. **105**	
	Medium Temperature	Temperature in°C.. **85**	
	Low Temperature	Temperature in°C.. **82**	
	Critical BW Level	Bandwidth level as % **3**	
	High BW Level	Bandwidth level as % **10**	
	Medium BW Level	Bandwidth level as % **100**	
	MEMHOT Level	[Disabled, Mid, Hi, **Critical**]	
	MEMTRIP	[**Disabled**]	
	Rx Skew Control	[**No Skew**, +2 Ticks, -2 Ticks]	
	TX Skew Control	[**No Skew**, +2 Ticks, -2 Ticks]	
	Performance Profile	[**17_19_13_18, 17_19_6_18, 17_19_6_7**]	
	Override Checkpoints	[**Auto,** Enabled, Disabled]	
	Scrambler	[Disabled, **Enabled**]	
	Slow Power Down Exit	[Disabled, **Enabled**]	
	Run/Boot Time Optimization		
	Skip memory test	[**Enabled,** Disabled]	
	Skip Command Training	[Enabled, **Disabled**]	
	SSA Config	VT-d	[**Enabled,** Disabled]
		VT-d Interrrupt remapp	[**Enabled,** Disabled]
		DFX Config.	Enables SSA Clock gating on Northbridge
South Bridge Chipset Configuration	SATA0 / SATA1 Configuration	Enable Controller	SATA Controller [Disabled, **Enabled**]
		SATA Testmode	SATA test mode [**Disabled**, Enabled]
		LPM	Link Power Management [**Disabled**, Enabled]
		Speed Limit	Indicated interface's highest available speed [Gen 1, Gen 2, **Gen 3**]
		Port Multiplier Support	Port multipler support for controller's Cap register [Disabled, **Enabled**]
		SATA0 Ports[1-7]	

Function	Second level Sub-Screen / Description			
South Bridge Chipset Configuration (continued)	SATA0 / SATA1 Configuration (continued)	Read Only Field Device Information and Device Size		
		Enable/Disable Port	SATA controller Port [Disabled, **Enabled**]	
		Hot Plug	Designates this port as Hot Pluggable. [Disabled, **Enabled**]	
		Spin up	Drivers that have this option spin up at boot. Otherwise all drives spin up at boot. [**Disabled**, Enabled]	
		Topology	Identified the SATA Topology [**Unknown,** ISATA, Direct Connect, Flex, M2]	
	USB Configuration	USB SS Configuration	Port 0 Port 1 Port 2 Port 3	Disabled = any USB devices plug into connector will not be detected by BIOS or OS [Disabled, **Enabled**]
		USB HS Configuration	Port 0 Port 1 Port 2 Port 3	disabled= any USB devices plug into connector will not be detected by BIOS or OS [Disabled, **Enabled**]
		USB Precondition	Precondition work on USB host controller and root ports for faster enumeration [**Disabled**, Enabled]	
		Inactivity Initiated	If programmed to non-zero, it allows L1 power managed to be enabled after the time-out period specified [Disabled, 32 bb_cclk, 64 bb_cclk, 128 bb_cclk, 256 bb_cclk, 512 bb_cclk, **1024 bb_cclk**, 131072 bb_cclk)	
		XHC Initiated L1	Sets XHC initiaded L1 power management [Disabled, **Enabled**]	
		XHCI Compliance Mode	Disable compliance mode [**Disabled**, Enabled]	
	PCIE IP Configuration	Bifurcation PCIe0	Selects and forces Root Complex Bifurcation configuration regardless of board or trident detection [**Auto**, x8, x4x4, x4x2x2, x2x2x4, x2x2x2x2]	
		Bifurcation PCIe1	Selects and forces Root Complex Bifurcation configuration regardless of board or trident detection [**Auto**, x8, x4x4, x4x2x2, x2x2x4, x2x2x2x2]	
		Compliance Test Mode	[**Disabled**, Enabled	
		Root Port [0 - 7]	Link Speed	Upper limit PCIe root port [Gen 1, Gen 2, **Gen 3**]

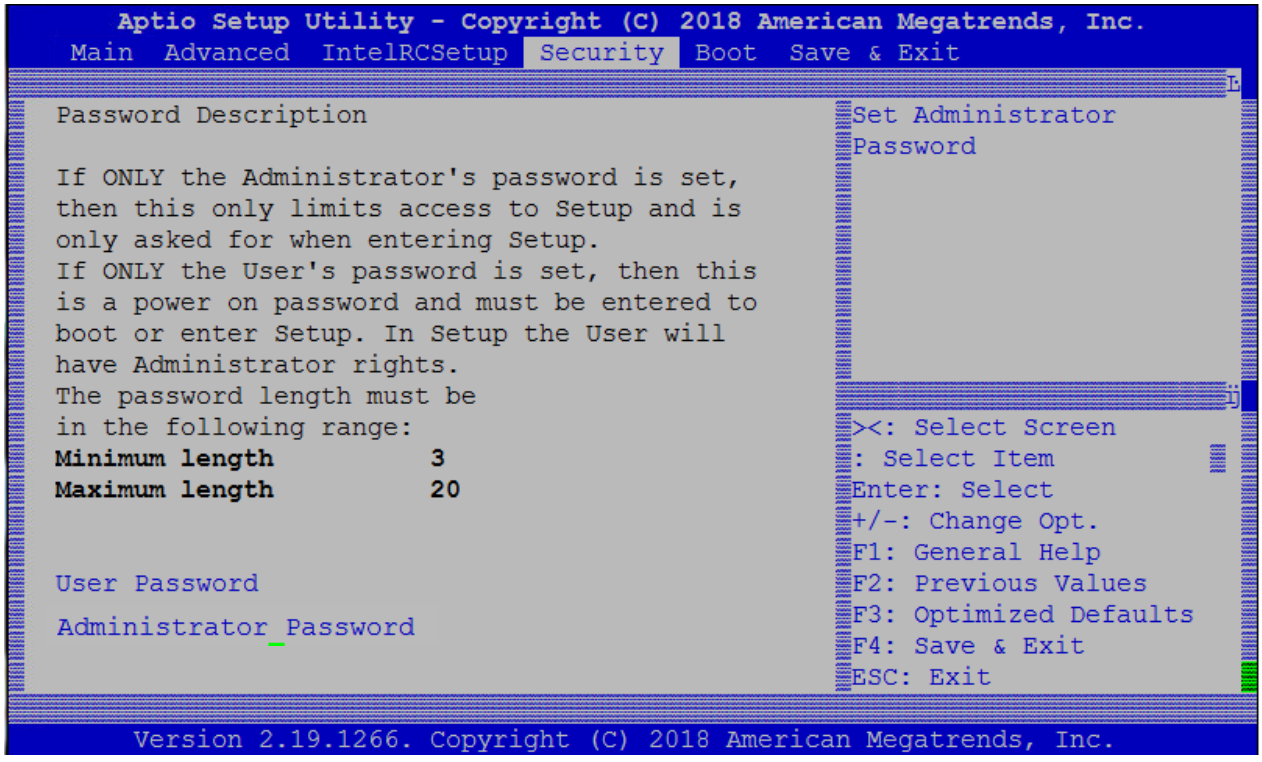
Function	Second level Sub-Screen / Description			
South Bridge Chipset Configuration (continued)	PCIE IP Configuration (continued)	Root Port [0 - 7] (continued)	Clock Gating	[Disabled, **Enabled**]
			Max. Payload	Set max. payload of PCIe Root Port or allow BIOS to select the value [128 Byte, 256 Byte, 512 Byte, 1024 Byte, 2048 Byte, 4096 Byte]
			Max. Read Request	Set Max.read request of PCIe Root Port or allow BIOS to select the value [**Auto**, 128 Byte, 256 Byte, 512 Byte, 1024 Byte, 2048 Byte, 4096 Byte]
			Extended Tag	If enabled device can use a 8-bit Tag field as requester [Disabled, **Enabled**]
			Relaxed Ordering	[**Disabled**, Enabled]
			Extended Synch	If enabled allows generation of Extended Synchronization patterns [**Disabled**, Enabled]
			De-Emphasis	At 5 Gb/s speed, this bit selects the level of de-emphasis for a downstream port. [-3.5 dB**, -6.0 dB**]
			Stop and Stream	[**Disabled**, Enabled]
			ASPM Support	Enable PCIe active stare power management settings [**L1**, Disabled]
			Surprise Link	Acive surprise link [Disabled, **Enabled**]
			RW-lock	Root port lock option [lock, unlock]
			Lane Reversal	Dynamic lane reversal on PCIe Root port [**Disabled**, Enabled]
			Completion Timeout Disable	[**Disabled**, Enabled]
			Completion Timeout Range	[Default, 50 us to 50 ms, 50 us to 100 ms,

Function	Second level Sub-Screen / Description			
South Bridge Chipset Configuration (continued)	PCIE IP Configuration (continued)	Root Port [0 - 7] (continued)	Completion Timeout Range (continued)	1 ms to 10 ms, 16 ms to 55 ms, **65 ms to 210 ms**, 260 ms, to 900 ms, 1 s to 3.5 s, 4 s to 13 s, 17 s to 64 s]
		Topology for PCIe Lane by Lane	Identifies PCIE Topology [SATA express, M2x4, M2x1, **x4**, x1, Unknown	
	PPM Config.	Enable and disable C-sate POPUP [Disabled, **Enabled**		
	State After G3	Specify state to go to when power re-applied after power failure (G3 state) [S0 state, S5 State, **Soft Strap**]		
	DCI Enable	DCI can debug over the USB 3 interface. When disabled, the host controller is not enabled [**Enabled**, Disabled]		
	SMBUS Controller	SMBUS Controller options [**Enabled**, Disabled]		
	SMBUS IOSFClockGating	SMBUS IOSFClockGating options [**Enabled**, Disabled]		
	SM Bus Host Speed	Indicates operating speed of physical bus [**Standard (80 KHz),** Standard (100 kHz), Fast mode (400 kHz), Fast mode plus (1 MHz)]		
	IOAPIC 24-119 Entries	OAPIC 24-119 Entries to expand to PIRQI-PIRQX [Enabled, **Disabled**]		
	GPIO Status	GPIO status help [Enabled, **Disabled**]		

12.2.4. Security Menu

The Security setup menu provides information about the passwords and functions for specifying the security settings.

Figure 14: Security Setup Menu



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

Table 34: Security Setup Menu Functions

Function	Description
User Password	Sets user password
Administrator Password	Sets administrator password

If only the administrator's password is set, access to the setup is limited and is requested when entering the setup.

If only the user's password is set, then the password is a power on password and must be entered to boot or enter setup. In the setup the user has administrator rights.

The required password length in characters is max. 20 and min. 3 and the passwords are case-sensitive.

12.2.4.1. Remember the Password

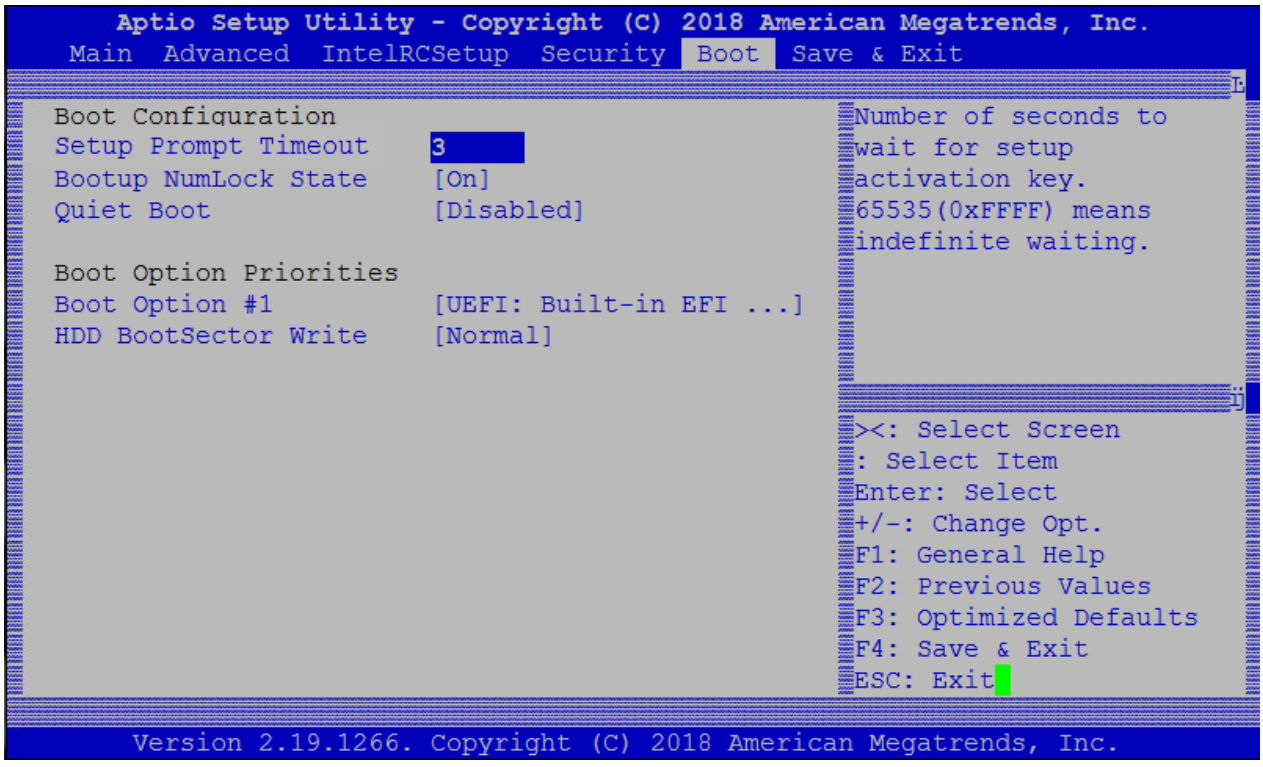
It is highly recommended to keep a record of all passwords in a safe place. Forgotten passwords results in the user being locked out of the system.

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.

12.2.5. Boot Menu

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

Figure 15: Boot Setup Menu



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

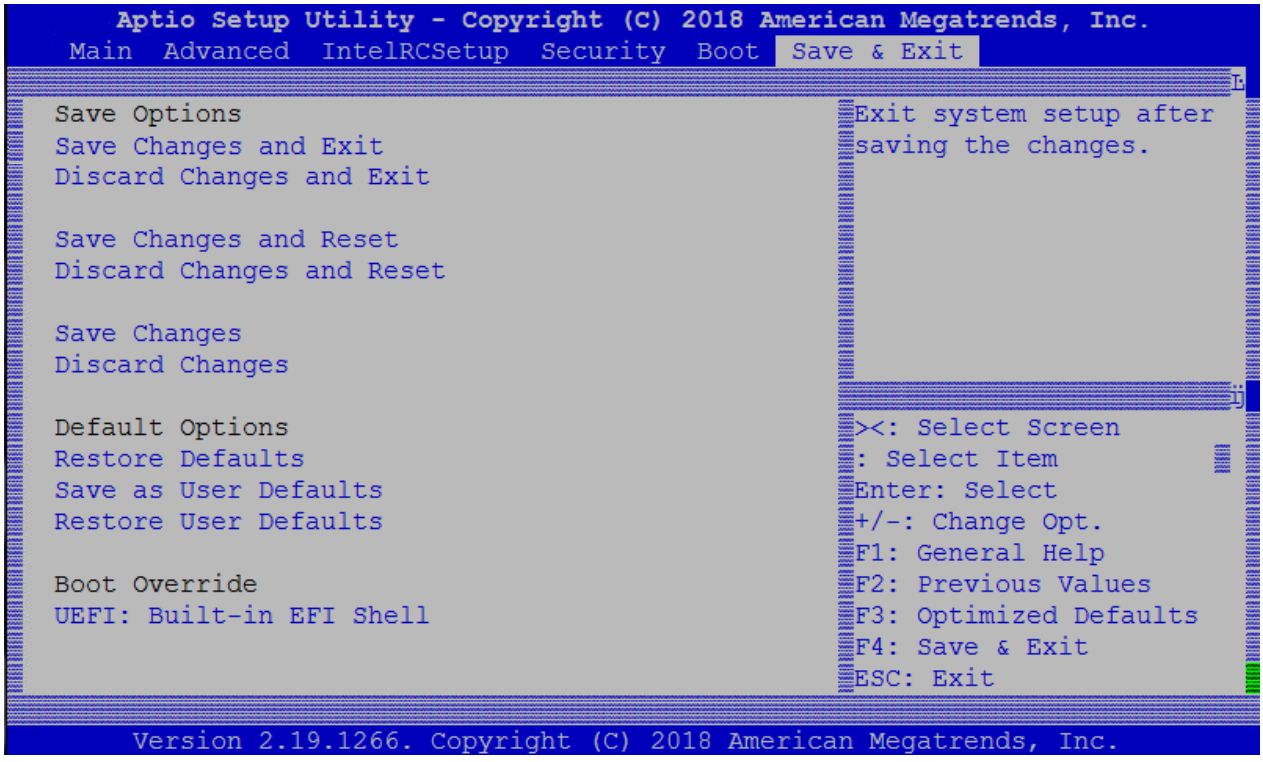
Table 35: Boot Setup Menu Functions

Function	Description
Boot Configuration	
Setup prompt Timeout	Displays number of seconds to wait for the setup activation key. 65535(OXFFF) means indefinite waiting [**3**]
Bootup NumLock State	Selects keyboard NumLock state [**On**, Off]
Quiet Boot	Enables or disables Quiet Boot [Enabled, **Disabled**]
Boot Option Priorities	
Boot Option #1	Sets the system boot order (option 1) [**UEFI Built-in EFI shell** Disabled]
HDD Boot sector Write	Enables or disables writes to hard disk sector 0 [**Normal**, Write protect]

12.2.6. Save and Exit

The Save and Exit setup menu lists the save, default and override options.

Figure 16: Save and Exit Setup Menu



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

Table 36: Save and Exit Menu Functions

Function	Description
Save Options	
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
Default 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
Boot Override Options	
UEFI Built-in EFI shell	Attempts to launch the built in EFI Shell

12.3. 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.

12.3.1. 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.

12.3.1.1. Entering the uEFI Shell

To enter the uEFI Shell, follow the steps below:

1. Power on the module.
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.

The output produced by the device mapping table can vary depending on the board's configuration.

If the <ESC> key is pressed before the 5 second timeout elapses, the shell prompt is shown:

```
Shell>
```

12.3.1.2. 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.

Appendix A: List of Acronyms

Table 37: List of Acronyms

ACPI	Advanced Configuration Power Interface
BIOS	Basic Input Output System
BSP	Board Support Package
CAN	Controller-area network
Carrier Board	Application specific circuit board that accepts a COM Express ® module
COM	Computer-on-Module
COMe-b	COM Express® b=basic 125 mm x 95 mm module form factor
COMe-c	COM Express® c=compact 95 mm x 95 mm module form factor
COMe-m	COM Express® m=mini 84 mm x 55 mm module form factor
COP	Computer Operating Properly
CPU	Central Processing Unit
DDC	Display Data Control
DDI	Digital Display Interface
DDIO	Digital Display Input/Output
DDR	
DIMM	Dual In-line Memory Module
DP	DisplayPort
DMA	Direct Memory Access
DMIC	Digital Microphone
DRAM	Dynamic Random Access Memory
DVI	Digital Visual Interface
EAPI	Embedded Application Programming Interface
ECC	Error Checking and Correction
EEPROM	Electrically Erasable Programmable Read-Only Memory
eDP	Embedded Display Port
EMC	Electromagnetic Compatibility (EMC)
eMMC	Embedded Multimedia Card
ESD	Electro Sensitive Device
FAT	File Allocation Table
Gb	Gigabit
GbE	Gigabit Ethernet
GPI	General Purpose Input
GPIO	General Purpose Input Output
GPO	General Purpose Output
GPU	Graphics Processing Unit
HDA	High Definition Audio (HD Audio)
HD/HDD	Hard Disk / Hard Disk Drive
HDMI	High Definition Multimedia Interface
HPM	PICMG Hardware Platform Management specification family
HWM	HardWare Monitor
IC	Integrated Circuit
I2C	Inter integrated Circuit Communications
I/O	Input /Output
IOT	Internet of Things
ISA	Industry Standard Architecture
JTAG	Joint Test Action Group
LAN	Local Area Network
LPC	Low Pin-Count Interface:
LPM	Link Power Management
LVDS	Low Voltage Differential Signaling –
MAC	Media Access Control
M.A.R.S.	Mobile Application for Rechargeable Systems
MLC	Multi Level Cell
MMIO	Main Memory Input Output
MTBF	Mean Time Before Failure
NA	Not Available
NC	Not Connected
NC-SI	Network Communications - Services Interface
NCQ	Native Command Queuing
NUMA	Non Uniform Memory Access
PCB	Plastic Circuit Board
PCH	Platform Controller Hub
PCI	Peripheral Component Interface
PCIe	PCI-Express
PEG	PCI Express Graphics
PICMG®	PCI Industrial Computer Manufacturers Group
PHY	Ethernet controller physical layer device

Pin-out Type	COM Express® definitions for signals on COM Express® Module connector pins.
pSLC	pseudo Single Level Cell
PSU	Power Supply Unit
RoHS	Restriction of the use of certain Hazardous Substances
RTC	Real Time Clock
S0	S0-Full power, all devices powered
S3	Suspend to RAM System context stored in RAM; RAM is in standby
S4	Suspend to Disk System context stored on disk
S5	Soft Off Main power rail off, only standby power rail present
SATA	Serial AT Attachment:
SFP	Small Form factor Pluggable
SLC	Single Level Cell
SMBus	System Management Bus

SoC	System on a Chip
SODIMM	Small Outline Dual In-line Memory Module
SPI	Serial Peripheral Interface
TOLUD	Top of Lower Useable DRAM
TOUUD	Top of Upper Useable DRAM
TPM	Trusted Platform Module
UART	Universal Asynchronous Receiver Transmitter
UEFI	Unified Extensible Firmware Interface
UHD	Ultra High Definition
USB	Universal Serial Bus
VT-d	Virtual Technology
VLP	Very Low Profile
WDT	Watch Dog Timer
WEEE	Waste Electrical and Electronic Equipment (directive)
XDP	eXtended Debug Port

About Kontron

Kontron is a global leader in embedded computing technology (ECT). As a part of technology group S&T, Kontron 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 S&T AG

Lise-Meitner-Str. 3-5
86156 Augsburg
Germany
Tel.: + 49 821 4086-0
Fax: + 49 821 4086-111
info@kontron.com