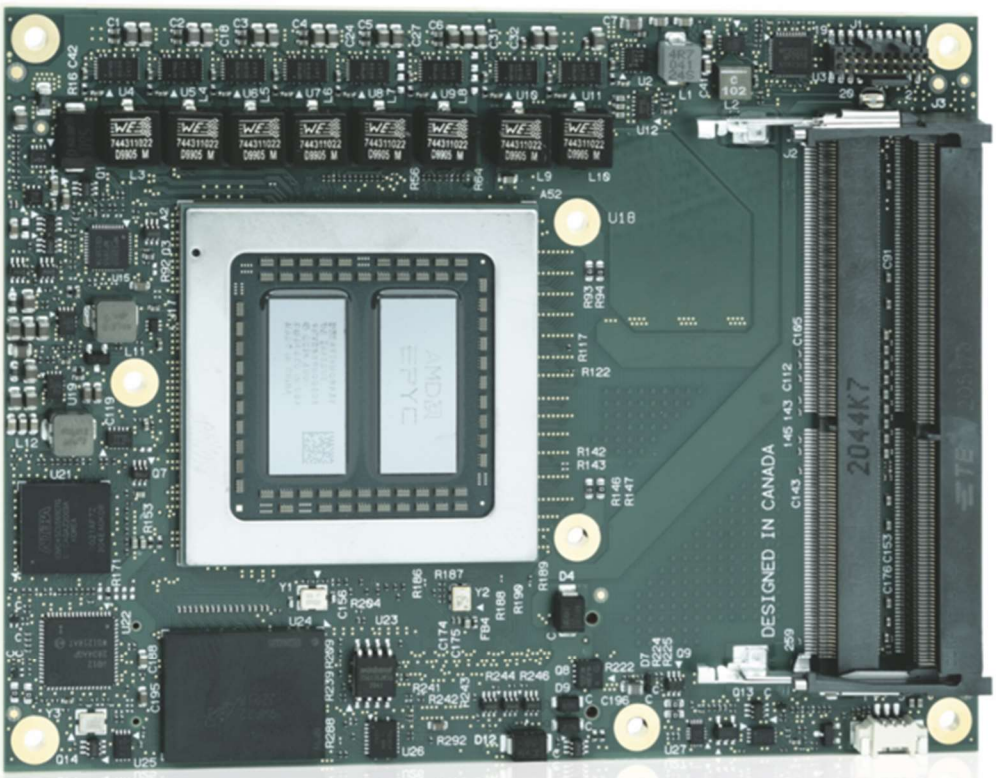
USER GUIDE



COMe-bEP7 Module

Doc.

Doc. ID: BEP7M102

This page has been intentionally left blank

COME-BEP7 MODULE - 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.

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

Revision History

Revision	Brief Description of Changes	Date of Issue	Author
0.1	Initial issue	2021 April 21st	MAG
1.01	Gate 4 document release	2022-02-08	MAG
1.02	Add notes to uEFI BIOS sections	2022-02-10	SH
1.03	Typo corrections	2022-04-19	MAG

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 manual

⚠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.
⚠CAUTION	CAUTION indicates a hazardous situation which, if not avoided, may result in minor or moderate injury.
NOTICE	NOTICE indicates a property damage message.
	Electric Shock! This symbol and title warn of hazards due to electrical shocks (> 60 V) when touching products or parts of them. 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. Please refer also to the "High-Voltage Safety Instructions" portion below in this section.
	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.

This symbol indicates general information about the product and the user manual.

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

1.1. Product Description

Kontron's Computer-on-Module COMe-bEP7 is a COM Express® BASIC TYPE 7 with AMD® EPYC®3000 PROCESSOR family with support for Pin-out Type 7, and an additional communication interface block. Kontron's module covers both the need for latest interface technology and the need to extend life-time. The AMD®

EPYC®3000 Generation increases efficiency and performance per watt ratio, which is a result of the innovative 14 nm technology and has up to 16 cores for control, micro server, storage and communication applications in Internet of Things (IoT) and embedded environment. The COMe-bEP7 is also designed for industrial temperature environment.

AMD® EPYC® 3000 Processor System on Chip (SoC),

Support Dual Die SP4

- DDR4 memory technology up to 32 GByte ECC Modules, 2x SODIMMs (4x SODIMMs optional)
- 64 high speed lanes connectivity:
  - 32x PCIE 3.0 (to COM Express Type 7)
  - 4x PCIE 3.0 to optional NVME oboard device
  - 1x PCIE 2.0 to i210 Ethernet controller.
  - QUAD 10 GbE interfaces
  - 2x SATA interfaces

Support Single Die SP4r2 SKUs

- DDR4 memory technology up to 32 GByte ECC Modules, 2x SODIMM only
- 32 PCIE 3.0 lanes:
  - high-speed connectivity of 24x PCIE 3.0 (to COM Express Type 7)
  - 1x PCIE 2.0 to i210 Ethernet controller
  - QUAD 10 GbE interfaces
  - 2x SATA interfaces

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 name for Kontron COM Express® Computer-On-Modules consists of:

Industry standard short form

- COMe-

Module form factor

- b=basic (125mm x 95mm)
- c=compact (95mm x 95mm)
- m=mini (84mm x 55mm)

AMD's processor code name

- EP = EPYC

Pinout type

- Type 7

Available temperature variants

- Commercial
- Industrial (E2)

Processor Identifier

- Chipset identifier (if chipset assembled)

Memory size

- Memory module (#G)

1.3. Understanding COM Express® Functionality

All Kontron COM Express® basic and compact modules contain two 220pin connectors; each of it has two rows called Row A & B on primary connector and Row C & D on secondary connector. The COM Express® Computer-On-Module (COM) features the following maximum amount of interfaces according to the PCI Industrial Computer Manufacturers Group (PICMG) module Pin-out type.

Table 1: Pin Assignment of Type 7 and COMe-bEP7

Feature	Type 7 Standard	COMe-bEP7 SP4 Pinout	COMe-bEP7 SP4r2 Pinout
Gbit Ethernet	1x	1x	1x
10GBaseKR Ethernet	4x	4x	4x
NC-SI	1x	1x	1x
PCI Express	32x	32x PCIe Gen3	24x PCIe Gen3
Serial ATA	2x	2x	2x
USB	4x USB 3.0 4x USB 2.0	4x USB 3.0 4x USB 2.0	4x USB 3.0 4x USB 2.0
Serial Ports	2x	2x	2x
LPC	1x	1x	1x
External SPI	1x	1x	1x
External SMB	1x	1x	1x
External I2C	1x	1x	1x
GPIO	8x	8x	8x

1.4. COM Express® Documentation

The COM Express® Specification defines the COM Express® module form factor, pin-out, and signals. This specification is available at the PICMG® website by filling out the order form.

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 baseboard that can accept present and future COM Express® modules.

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

A single baseboard design can use a range of COM Express® modules with different sizes and pinouts. 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® baseboard can work with several successive generations of COM Express® modules.

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

2/ Product Specification

2.1. Module Definition

The COM Express® basic sized Computer-on-Module COMe-bEP7 (bEP7) follows pin-out Type 7 and is compatible to PICMG specification COM.0 Rev 3.0. The COMe-bEP7 is available in different variants to cover the different demands in performance, price and power.

2.2. Commercial Grade Modules

The following is a list of modules for commercial temperature range.

Table 2: Commercial Grade Modules (0°C to 60°C operating)

Product Number	Product Name	Description
68010-0000-51-3	COMe-bEP7 E3351	COM Express® basic pin-out type 7 Computer-on-Module with AMD® EPYC® 3000 Processor E3351, 12 core, Quad 10GbE, 1x GbE, 2x DDR4 non-ECC/ECC SO-DIMM
68010-0000-51-4	COMe-bEP7 E3451	COM Express® basic pin-out type 7 Computer-on-Module with AMD® EPYC® 3000 Processor E3351, 16 core, Quad 10GbE, 1x GbE, 2x DDR4 non-ECC/ECC SO-DIMM
68010-0000-61-4	COMe-bEP7 E3451	COM Express® basic pin-out type 7 Computer-on-Module with AMD® EPYC® 3000 Processor E3351, 16 core, Quad 10GbE, 1x GbE, 4x DDR4 non-ECC/ECC SO-DIMM
68010-0000-51-1	COMe-bEP7 E3151 10K	COM Express® basic pin-out type 7 Computer-on-Module with AMD® EPYC® 3000 Processor E3151, 2 core, Quad 10GbE, 1x GbE, 2x DDR4 non-ECC/ECC SO-DIMM
68010-0000-51-2	COMe-bEP7 E3251 10K	COM Express® basic pin-out type 7 Computer-on-Module with AMD® EPYC® 3000 Processor E3251, 4 core, Quad 10GbE, 1x GbE, 2x DDR4 non-ECC/ECC SO-DIMM

2.3. Industrial Grade Modules

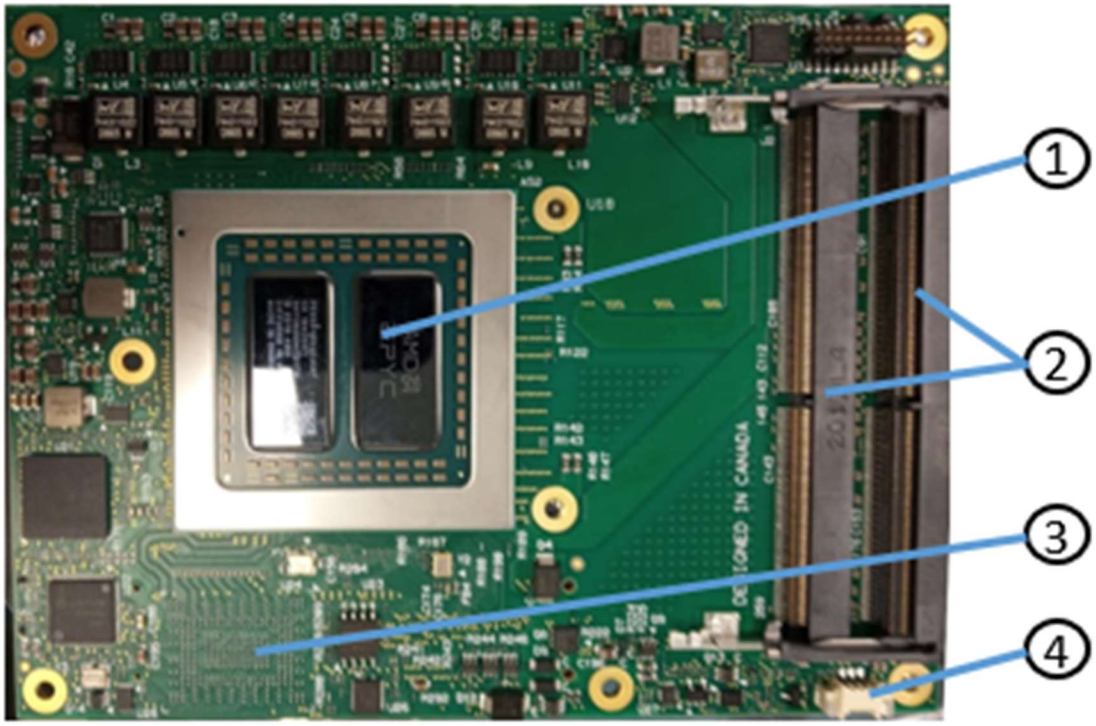
Industrial temperature grade modules are available based on their design. Please contact your local sales or support for further details.

Table 3: Industrial Grade Modules by Design (E2, -40°C to 85°C Operating)

Product Number	Product Name	Description
68011-0000-55-2	COMe-bEP7R E2 E3255	COM Express® basic pin-out type 7 Computer-on-Module with AMD® EPYC® 3000 Processor E3255, 8 Core, QUAD 10GbE (KR), 1x GbE, 2x DDR4 non-ECC/ECC SO-DIMM

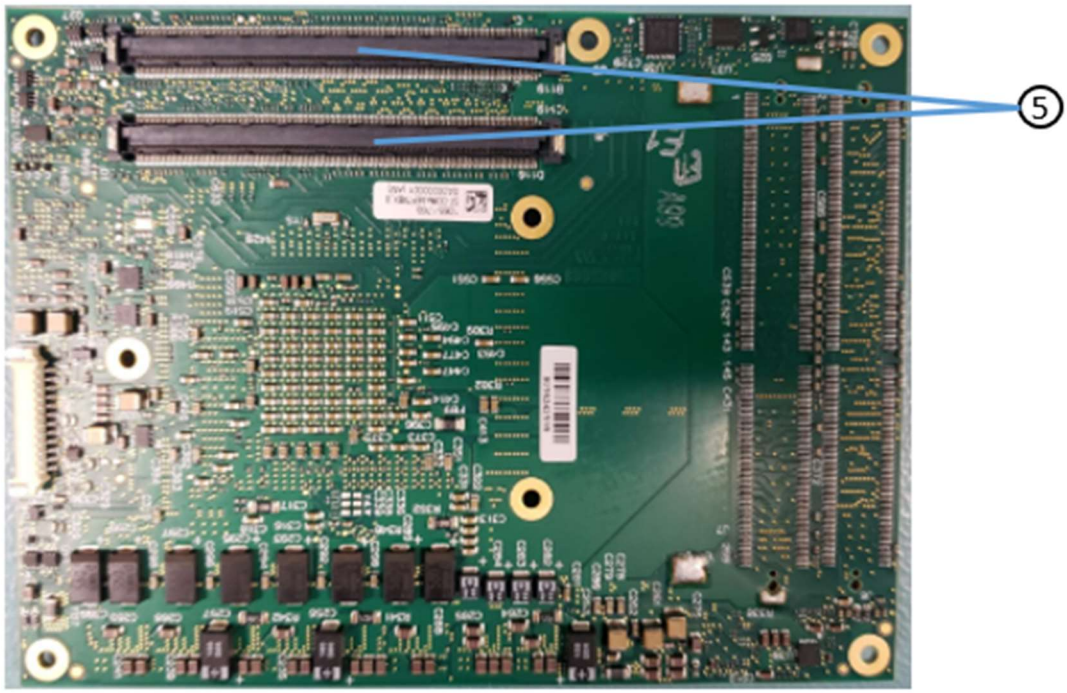
2.4. Product Views

Figure 1: Top View of COMe bEP7



1. Processor
2. 2x DDR4 memory
3. Onboard NVME
4. Fan Connector

Figure 2: Bottom View of COMe bEP7



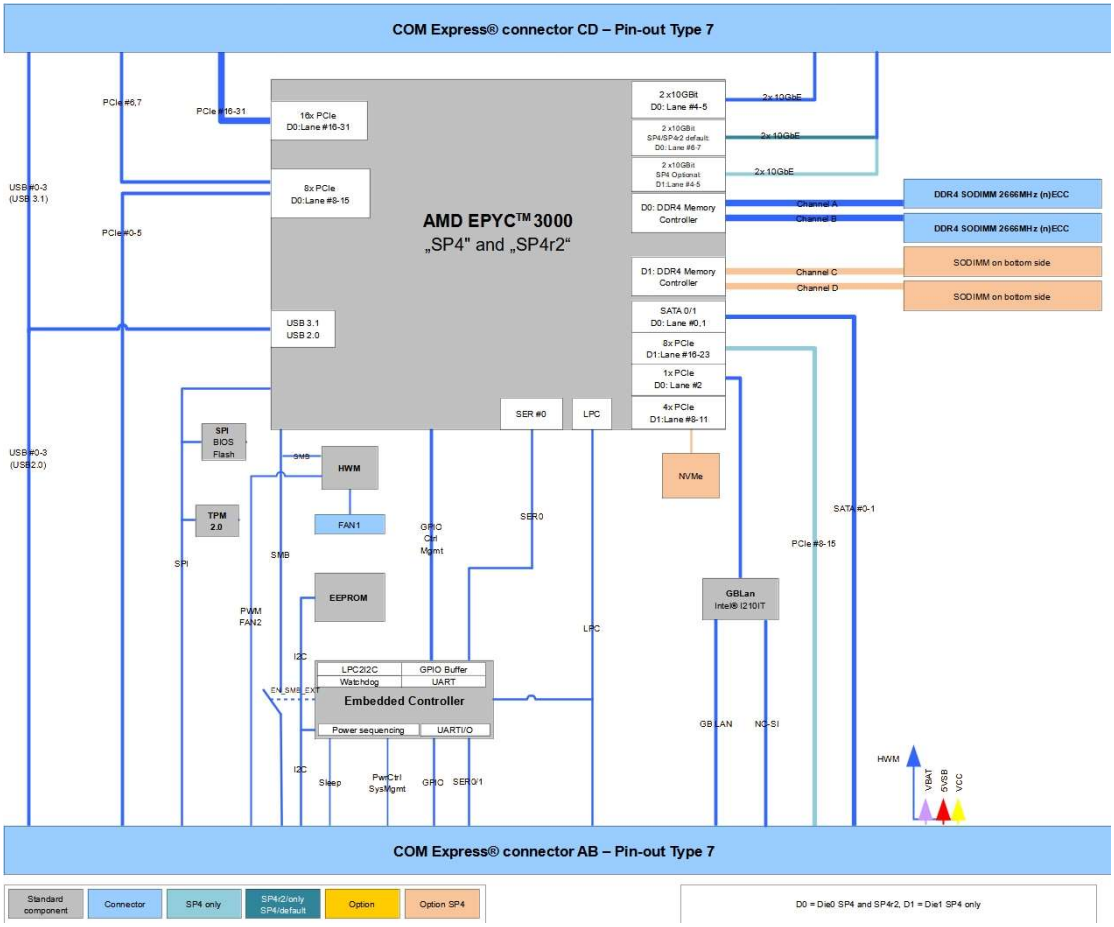
5. 2x COMe interfaces

3/ Functional Specification

3.1. Block Diagram COMe-bEP7

Figure 3 displays the block diagram applicable to all COMe-bEP7 modules.

Figure 3: Block Diagram COMe-bEP7, basic pinout with AMD EPYC 3000 SP4 and SP4r2 Processor Family SoC



3.2. Processor

AMD EPYC™ Embedded 3000 processors expand the AMD EPYC™ Embedded family of products to harness the breakthrough performance benefits of the “Zen” CPU architecture, bringing exceptional reliability, availability and serviceability features to networking, storage and industrial applications. Leveraging major advancements in I/O integration, flexibility, and security capabilities.

Performance

- 4, 8, 12, 16 core per socket
- 40 PCIe Gen3 lanes
- 4x 10 GBe
- 4 Memory Channel

Reliability Availability Serviceability (RAS) includes:

- Low-SER FinFET Transistors
- Parity and error-tolerant devices throughout core
- Caches
  - L1 data cache with SEC-DED ECC
  - L1 data tag / L1 instruction cache with parity + retry
  - L2 / L3 caches with DEC-TED ECC
- DRAM
  - DRAM ECC with Chipkill capabilities
  - DRAM Address/Command Parity with Replay
  - DRAM Write Data CRC with Replay
- CRC protection of core CC6 state
- Parity on all internal data buses
- Link Packet CRC with Retry
- Sync Flood on uncontainable errors
- PCIe® Advanced Error Recovery (AER)
- PCIe® Downstream Port Containment (DPC)

Advanced Security Features

- AMD EPYC™ Embedded 3000 processors feature an onboard AMD Secure Processor that encrypts data before it feeds to the I/O, complemented with Hardware Validated Boot capabilities to help ensure systems are booting from trusted software, with one-time programmable (OTP) capabilities enabling system designers' unique configuration. Advanced capabilities include Secure Memory Encryption (SME) for helping defend against unauthorized memory access, and Secure Encrypted Virtualization (SEV) for helping isolate hypervisors and virtual machines (VMs) – with no application code changes required

Table 4: AMD EPYC® Embedded 3000 Product Family Specifications

	SP4		SP4r2				
AMD EPYC® Processor	E3351	E3451	E3101	E3151	E3201	E3251	E3255
# of Cores	12	16	4	4	8	8	8
# of Threads	24	32	4	8	8	16	16
Base Freq.	1.9	2.45	2.1	2.7	1.5	2.5	2.0 / 2.5
Turbo Frequency (GHz)	3.0	3.0	2.9	2.9	3.1	3.1	3.1
Thermal Design Power (TDP) (W)	65-80	85-100	35	45	30	55	30-55
Command	64Bit	64Bit	64Bit	64Bit	64Bit	64Bit	64Bit
Cache (MB)	6/32	8/32	2/8	2/16	4/16	4/16	4/16
Memory Type	DDR4-2666	DDR4-2666	DDR4-2666	DDR4-2666	DDR4-2666	DDR4-2666	DDR4-2666
Max Memory Size (GB) with SODIMM	128 (4x 32)[1]	128 (4x 32)[1]	64 (2x 32)[1]	64 (2x 32)[1]	64 (2x 32)[1]	64 (2x 32)[1]	64 (2x 32)[1]
ECC Memory	Yes	Yes	Yes	Yes	Yes	Yes	Yes
PCIe Express (to Type 7 connectors)	32x	32x	24x	24x	24x	24x	24x

[1] on the COMe-bEP7 SP4 SKU, two SODIMM sockets are supported by default for a max of 2x 32 GB memory. Four SODIMM sockets optional.

3.3. Memory

Table 5: Memory Features

Socket	2x DDR4 SO-DIMM (default) 4x DDR4 SO-DIMM (Optional with SP4 SKUs)
Memory Type	Dual/QUAD Channel DDR4, up to 2666 MT/s, up to 32 GB per socket
Memory Module Size	8 GByte, 16 GByte and 32 GByte

3.4. USB

USB 3.0 ports are backwards compatible with the USB 2.0 specification. The COMe-bEP7 allows a maximum of four USB 3.0 (USB 2.0) ports.

Table 6: Supported USB Features

USB 3.0 Ports	up to 4x USB 3.0
USB 2.0 Ports	up to 4x USB 2.0
USB Over Current Signals	2x

3.5. PCI Express Configuration

The EPYC 3000 processor has up to 64 high speed lanes from the SoC, used for PCIe, SATA and Ethernet. On SP4 SKUs all 32 lanes to COMe interface are available. With SP4r2 only 24 lanes are available (Lanes 8 to 15 are not used).

- COMe PCIe #0 to COMe PCIe #7 can be bifurcated in x8, x4, x2, or x1.
- COMe PCIe #8 to COMe PCIe #15 can be bifurcated in x8, x4, x2, or x1. Only available with SP4 (dual Die).
- COMe PCIe #16 to COMe PCIe #31 can be bifurcated in x16 , x8 or x4.

3.5.1. AMD restrictions associated with the links

- There are a maximum of 8 PCIe ports in any x16 link. A x16 link cannot be connected to more than 8 PCIe devices.
- Any 8 lane subset (lanes [15:8] or [7:0]) of a x16 link cannot be configured to contain more than 7 ports.
- All PCIe links that are a subset of a given x16 link must be aligned to their natural bit boundaries. For example,
  - x8 links can only contain lanes [15:8] and [7:0].
  - x4 links can only contain lanes [15:12], [11:8], [7:4] and [3:0].
  - x2 links can only contain lanes [15:14], [13:12], [11:10], [9:8], [7:6], [5:4], [3:2], [1:0].

3.5.2. Enabling COMe-bEP7 PCIe Links Configuration

Setup Options are available in the BIOS Menu for PCIe Links Configuration in BIOS menu.

UEFI Setup Menu: Advanced → AMD PBS

Table 7: PCIe Biffurcation Table

Function	Second level Sub-Screen / Description	Description
COMe PCIE[0:7] Lanes		Limitation to maximum 7 ports.
Link Width at PCIE0	[Disabled, x1, 2, x4, **x8**]	Number of PCIE lanes for Link starting at COMe PCIE0.
Link Width at PCIE1	[**Disabled**, x1]	Number of PCIE lanes for Link starting at COMe PCIE1.
Link Width at PCIE2	[**Disabled**, x1, x2]	Number of PCIE lanes for Link starting at COMe PCIE2.
Link Width at PCIE3	[**Disabled**, x1]	Number of PCIE lanes for Link starting at COMe PCIE3.
Link Width at PCIE4	[**Disabled**, x1, x2, x4]	Number of PCIE lanes for Link starting at COMe PCIE4.
Link Width at PCIE5	[**Disabled**, x1]	Number of PCIE lanes for Link starting at COMe PCIE5.
Link Width at PCIE6	[**Disabled**, x1, x2]	Number of PCIE lanes for Link starting at COMe PCIE6.
Link Width at PCIE7	[**Disabled**, x1]	Number of PCIE lanes for Link starting at COMe PCIE7.
COMe PCIE[8:15] Lanes		SP4 only Limitation to maximum 7 ports.
Link Width at PCIE8	[Disabled, x1, 2, x4, **x8**]	Number of PCIE lanes for Link starting at COMe PCIE8.
Link Width at PCIE9	[**Disabled**, x1]	Number of PCIE lanes for Link starting at COMe PCIE9.
Link Width at PCIE10	[**Disabled**, x1, x2]	Number of PCIE lanes for Link starting at COMe PCIE10.
Link Width at PCIE11	[**Disabled**, x1]	Number of PCIE lanes for Link starting at COMe PCIE11.
Link Width at PCIE12	[**Disabled**, x1, x2, x4]	Number of PCIE lanes for Link starting at COMe PCIE12.
Link Width at PCIE13	[**Disabled**, x1]	Number of PCIE lanes for Link starting at COMe PCIE13.
Link Width at PCIE14	[**Disabled**, x1, x2]	Number of PCIE lanes for Link starting at COMe PCIE14.
Link Width at PCIE15	[**Disabled**, x1]	Number of PCIE lanes for Link starting at COMe PCIE15.
COMe PCIE[16:31] Lanes		
Link Width at PCIE16	[Disabled, x4, x8, **x16**]	Number of PCIE lanes for Link starting at COMe PCIE0.
Link Width at PCIE20	[**Disabled**, x4]	Number of PCIE lanes for Link starting at COMe PCIE1.
Link Width at PCIE24	[**Disabled**, x4, x8]	Number of PCIE lanes for Link starting at COMe PCIE2.
Link Width at PCIE28	[**Disabled**, x4]	Number of PCIE lanes for Link starting at COMe PCIE3.

3.6. SATA

The SATA high-speed storage interface supports two SATA Gen.3 ports with transfer rates of up to 6 Gb/s.

Table 8: COMe Connector Port and SoC Port Combinations for SATA

COMe Port	Comment
SATA_0	SATA Gen.3, 6 Gb/s
SATA_1	SATA Gen.3, 6 Gb/s

3.7. Ethernet

The COMe-bEP7 offers the following Ethernet Controllers:

1Gbe:

One Intel® Ethernet I210 Controller

10 Gbe:

SP4 SKUs:

- AMD® EPYC SoC QUAD Ethernet 10GbE Controller

SP4r2 SKUs:

- AMD® EPYC SoC QUAD Ethernet 10GbE Controller

3.7.1. Supported modes

The 10GbE interface can be configured in three different modes in the UEFI menus. Setting configuration are detailed in section: “AMD CBS Sub-Menu” items related to “XGBE” settings.

- KR (Backplane application)
- SFP+ DAC (Direct Attached Cable)
- SFP+ (with KR/SFI PHY)

3.7.1.1. KR:

10GBASE-KR for GbE backplane applications (IEEE802.3 clause 72)

Auto-negotiation for backplane Ethernet (IEEE 802.3 Clause 73)

3.7.1.2. SFP+(DAC):

Tested with Kontron carrier boards. Customer implementation is not advised and would require carrier integration and drive setting tuning. Please contact your local sales or support for further details.

3.7.1.3. 10Gb KR/SFP+:

An external PHY is required.

Tested with CS4223/CS4227 Inphy phys.

3.7.1.4. 10G Base-T

AMD POR support 88x3310 phy from Marvell. There is no evaluation carrier available from Kontron for this mode.

Refer to table below for associated carrier boards and adaptors:

Table 9: 10G modes evaluation carrier configurations

10G mode	GEN 1 carrier config (68300-0000-00-0)	GEN 2 carrier config (68301-0000-00-8)
KR	Direct connection using passive copper modules	Needs: 68301-0000-04-4 DAC adaptor
SFP+ (DAC)	Direct connection using passive copper modules	Needs: 68301-0000-04-4 DAC adaptor
KR/SFP+	Not available on carrier	Needs: 68301-0000-3-2 Dual port (CS4227) 68301-0000-3-4 Quad port (CS4223)
10GBase-T	Not available on carrier	Not available on carrier

3.7.2. I210 1GbE

The I210 controller has the following features:

Platform Power Efficiency
IEEE 802.3az Energy Efficient Ethernet (EEE)
Proxy: ECMA-393 and Windows* logo for proxy offload

The SoC embedded ports have the following features:
IEEE 802.3 specification Clauses 49, 72, and 73.

Manageability:

Preboot Execution Environment (PXE) and Internet Small Computer System Interface (iSCSI) boot

Broad OS Support and Validation:

Windows, VMWare and Linux(Ubuntu)

Unified networking:

NOTICE

Please download application note from EMD Customer Section.
Please contact your local sales or support for further details

3.8. COMe Features

The following table lists the supported COM Express® features.

Table 10: COMe Features

SPI	Boot from an external SPI
LPC	Supported
UART	2x UART (RX/TX)
Sleep Signals	Supported
SMBus	Speed configurable, default 100 k SMB

3.9. Kontron Features

The following table lists the supported Kontron specific product features.

Table 11: Kontron Features

External I2C Bus	Fast I2C, Multimaster capable
Embedded API	KeAPI 3.0 for all supported OS
Customer BIOS Settings / Flash Backup	Supported
Watchdog Support	3 stage
External SIO	Supported on the base board (with customized BIOS)
GPIO	Start-up level configurable, GPI interrupt capable

4/ Accessories

4.1. Product Specific Accessories

Table 12: Product Specific Accessories List

Product Number	Product	Description
68300-0000-00-0	COMe Eval Carrier T7	COM Express® Eval Carrier Type 7 GEN 1
68301-0000-00-8	COMe Eval Carrier T7 GEN2	COM Express® Eval Carrier Type 7 GEN2
68301-0000-03-4	ADA-COME-T7-G2 4X10G SFP+-DEV-TOOL	COMe Type 7 Adapter Card, 4x 10GbE SFP+ adapter with CS4223 Phy to be used in combination with COMe Eval Carrier T7 GEN 2
68301-0000-03-2	ADA-COME-T7-G2 2X10G SFP+-DEV-TOOL	COMe Type 7 Adapter Card, 2x 10GbE SFP+ with CS4227 Phy adapter to be used in combination with COMe Eval Carrier T7 GEN 2
68301-0000-04-4	ADA-COMe-T7-G2 4x10G DAC - DEV-TOOL	COMe Type 7 Adapter Card, 4x 10GbE Direct Attached Connection to SFP+ adapter to be used in combination with COMe Eval Carrier T7 GEN 2
68011-0000-99-0	HSP COMe-bEP7 thread	Heatspreader for COMe-bEP7, threaded mounting holes
68011-0000-99-1	HSP COMe-bEP7 through	Heatspreader for COMe-bEP7, through holes
68002-0000-99-0C06	HSK COMe-bBD6 passive (w/o HSP)	Passive Cooler for COMe-bBD6/COMe-bEP7 to be mounted on HSP
68002-0000-99-0C05	HSK COMe-bBD6 active (w/o HSP)	Active Cooler for COMe-bBD6/bEP7 to be mounted on HSP
97030-0827-BEP7	DDR4-2666 8 GByte ECC	DDR4-2666, 8GB, ECC, 260P, 1333MHz, PC4-22666 SODIMM
97030-1627-BEP7	DDR4-2666 16 GByte ECC	DDR4-2666, 16GB, ECC, 260P, 1333MHz, PC4-2666 SODIMM
97030-3227-BEP7	DDR4-2666 32 GByte ECC	DDR4-2666, 16GB, ECC, 260P, 1333MHz, PC4-2666 SODIMM

97031-0827-BEP7	DDR4-2666 8 GByte E2 ECC	DDR4-2666, 8GB, ECC, E2, 260P, 1333MHz, PC4-2666 SODIMM
97031-1627-BEP7	DDR4-2666 16 GByte E2 ECC	DDR4-2666, 16GB, ECC, E2, 260P, 1333MHz, PC4-2666 SODIMM
97031-3227-BEP7	DDR4-2666 32 GByte E2 ECC	DDR4-2666, 16GB, ECC, E2, 260P, 1333MHz, PC4-2666 SODIMM

4.2. General Accessories

Table 13 provides a list of general accessories applicable to all COMe pin-out Type 7 products.

Table 13: General Accessories List

Product Number	Mounting	Description
38017-0000-00-5	COMe Mount KIT 5mm 1set	Mounting Kit for 1 module including screws for 5mm connectors
38017-0000-00-0	COMe Mount KIT 8mm 1set	Mounting Kit for 1 module including screws for 8mm connectors
Product Number	**Cables**	**Description**
96079-0000-00-0	KAB-HSP 200mm	Cable adapter to connect Fan to module (COMe basic/compact)
96079-0000-00-2	KAB-HSP 40mm	Cable adapter to connect Fan to module (COMe basic/compact)

5/ Electrical Specification

5.1. Supply Voltage

Table 14 provides information regarding the supply voltage specified at the COM Express® connector.

Table 14: COM Express® Connector Electrical Specifications

	Commercial Grade	Industrial Grade
VCC	8.5 V – 20 V	12 V
Standby	5V DC +/- 5% (5 VSB is not mandatory for operation)	5 V DC +/- 5%
RTC	2.8 V - 3.47 V	2.8 V - 3.47 V

5 V Standby voltage is not mandatory for operation.

5.2. Power Supply Rise Time

The input voltages should rise from ≤10% of nominal to within the regulation ranges within 0.1 ms to 20 ms.

There must be a smooth and continuous ramp of each DC input voltage from 10% to 90% of its final set-point following the ATX specification.

5.3. Supply Voltage Ripple

Maximum 100 mV peak to peak 0 – 20 MHz.

5.4. Power Consumption

The maximum Power Consumption of the different COMe-bEP7 variants is 35 W to 100 W (100% CPU load on all cores; 90°C CPU temperature).

For Information on Detailed Power Consumption measurements in all states and benchmarks for CPU, Graphics and Memory performance, refer to the Application Note at EMD Customer Section.

5.5. ATX Mode

By connecting an ATX power supply with VCC and 5VSB, PWR_OK is set to low level and VCC is off. Press the Power Button to enable the ATX PSU setting PWR_OK to high level and powering on VCC. The ATX PSU is controlled by the PS_ON# signal which is generated by SUS_S3# through inversion. VCC can be 8.5 V – 20 V in ATX Mode. On Computer-on-Modules supporting a wide range input down to 4.75 V the input voltage shall always be higher than 5 V Standby (VCC > 5VSB).

Table 15: ATX Mode

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

5.6. Single Supply Mode

In single supply mode, without 5V standby the module will start automatically when VCC power is connected and Power Good input is open or at high level (internal PU to 3.3V). VCC can be 8.5 V – 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.

Table 16: Single Supply Mode

State	PWRBTN#	PWR_OK	V5_StdBy	VCC
G3	0	0	0	0
G3 → S0	high	open / high	OPEN	connecting VCC
S5	high	open / high	OPEN	VCC
S5 → S0	PWRBTN Event	open / high	OPEN	reconnect VCC

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

NOTICE

If any of the supply voltages drops below the allowed operating level longer than the specified hold-up time, all the supply voltages should be shut down and left OFF for a time long enough to allow the internal board voltages to discharge sufficiently.
If the OFF time is not observed, parts of the board or attached peripherals may work incorrectly or even suffer a reduction of MTBF.

The minimum OFF time depends on the implemented PSU model and other electrical factors and needs to be measured individually for each case.

6/ Power Control

6.1. Power Supply

The COMe-bEP7 supports a power input from 8.5 V to 20 V in the commercial grade version, but 12 V in the industrial version. The supply voltage is applied through the VCC pins (VCC) of the module connector.

Optionally, 5 V +/- 5% can be applied to the V_5V_STBY pins and allows support for wake-up suspend-to-disk and soft-off state when the VCC power is removed.

Suspend-to-RAM (S3) is not supported by the AMD EPYC product family.

6.2. Power Button (PWRBTN#)

The power button (Pin B12) is available through the module connector described in the pin-out list. To start the module using Power Button the PWRBTN# signal must be at least 50ms (50 ms ≤ t < 4 s, typical 400 ms) at low level (Power Button Event).

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

6.3. Power Good (PWR_OK)

The COMe-bEP7 provides an external input for a power-good signal (Pin B24). The implementation of this subsystem complies with the COM Express® Specification. PWR_OK is internally pulled up to 3.3 V and must be high level to power on the module. This is typically driven by the ATX power supply PWR_OK signal. The carrier needs to release the signal when ready.

6.4. Reset Button (SYS_RESET# Signal)

When the SYS_RESET# pin is detected active, 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 to 6 ms regardless of whether the SYS_RESET# input remains asserted or not.

6.5. SM-Bus Alert (SMB_ALERT#)

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

7/ Environmental Specification

7.1. Temperature Specification

Kontron defines following temperature grades for Computer-on-Modules in general. Please see chapter 'Product Specification' for available temperature grades for the COMe-bEP7.

Table 17: General Temperature Specification

Temperature Specification	Operating	Non-operating
Commercial grade	0°C to +60°C	-30°C to +85°C
Industrial grade by Design (E2)	-40°C to +85°C	-40°C to +85°C

7.2. Operating with Kontron heatspreader plate assembly

The operating temperature defines two requirements:

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

Table 18: Test Specification

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

7.3. Operating without Kontron heatspreader plate assembly

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

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

7.4. Standards and Certifications

- RoHS II: The COMe-bEP7 is compliant to the directive 2011/65/EU on the Restriction of the use of certain Hazardous Substances (RoHS II) in electrical and electronic equipment.

Figure 4: RoHS

Component Recognition UL 60950-1

The COM Express® basic form factor Computer-on-Modules are Recognized by Underwriters Laboratories Inc.

Representative samples of this component have been evaluated by UL and meet applicable UL requirements.

CE

CE according to

EN62368-1:2014 + AC:2015
EN610000-6-3:2005 + Cor:2005
CISPR 22: Edition 6.0 2008-09
CISPR 32: 2015
EN55022:2010+AC:2011
EN55024:2010

UL Listings:

NWGQ2.E304278
NWGQ8.E304278

Figure 5: Component Recognition UL

WEEE Directive

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

Conformal Coating

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

Shock & Vibration

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

IEC/EN 60068-2-6 (Non operating Vibration, sinusoidal, 10 Hz to 2000 Hz, +/-0.15 mm, 2 g)

IEC/EN 60068-2-27 (Non operating Shock Test, half-sinusoidal, 11 ms, 15 g)

EMC

Validated in Kontron reference housing for EMC the COMe-bEP7 follows the requirements for electromagnetic compatibility standards:

EN55022

EN55024

2004/108/EC

FCC Part 15

MTBF

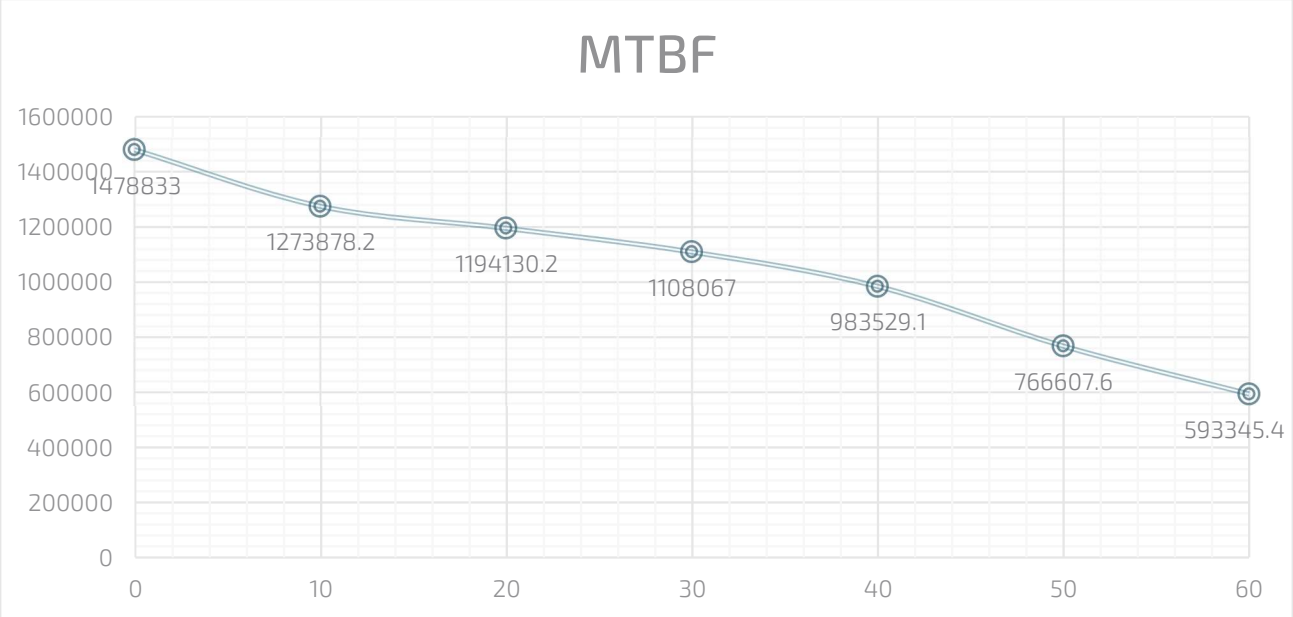
The following MTBF (Mean Time Before Failure) values were calculated using a combination of manufacturer's test data, if the data was available, and the Telcordia (Bellcore) issue 2 calculation for the remaining parts.

The Telcordia calculation used is "Method 1 Case 3" in a ground benign, controlled environment (GB,GC). This particular method takes into account varying temperature and stress data and the system is assumed to have not been burned in. or 62 years

Figure 6 shows MTBF de-rating for the E1 temperature range in an office or telecommunications environment. Other environmental stresses (such as extreme altitude, vibration, salt water exposure) lower MTBF values.

System MTBF (hours) = 983529 h @ 40°C or 62 years

Figure 6: MTBF Temperature De-rating for Product 68010-0000-51-3 COMe-bEP7R with D-E3351 Processor



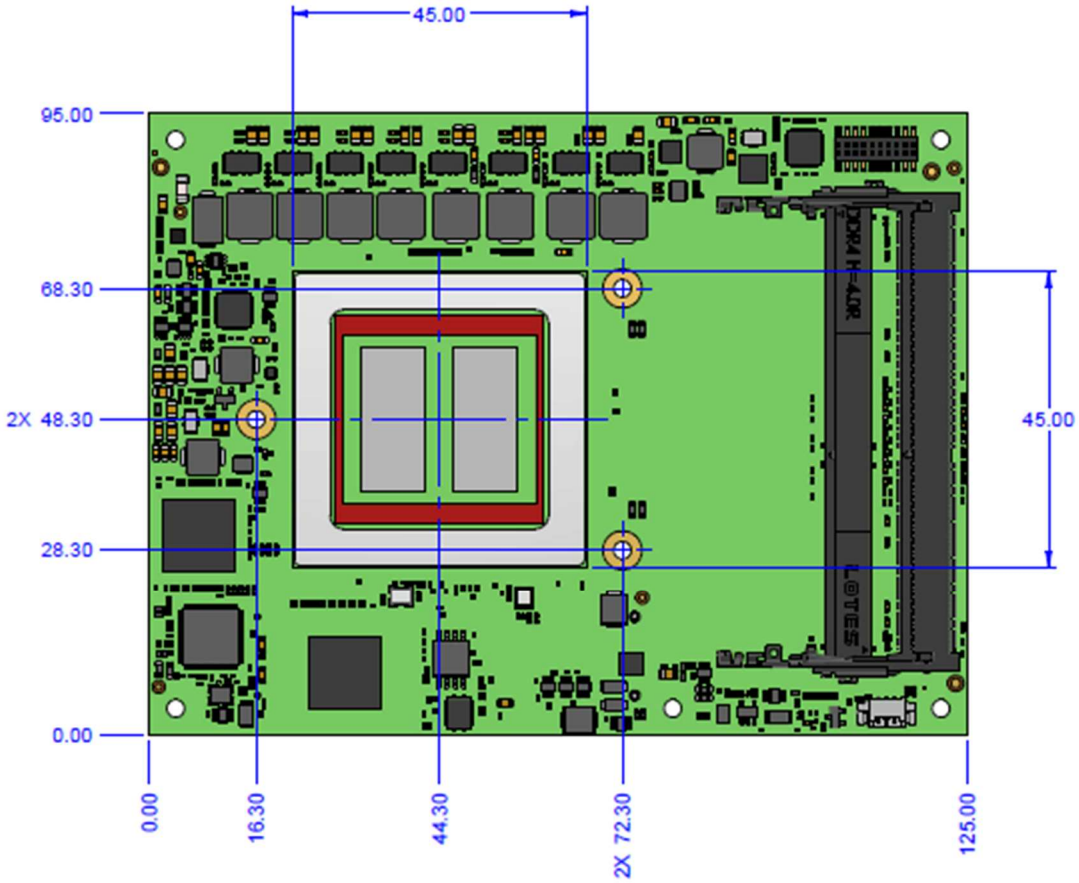
The above estimates assume no fan, but a passive heat sinking arrangement. Estimated RTC battery life (as opposed to battery failures) is not accounted for in the above figure and needs to be considered for separately. Battery life depends on both temperature and operating conditions. When the Kontron unit has external power; the only battery drain is from leakage paths.

8/ Mechanical Specification

8.1. Dimensions

The dimensions of the module are 95.0 mm x 125.0 mm.

Figure 7: Module Dimensions



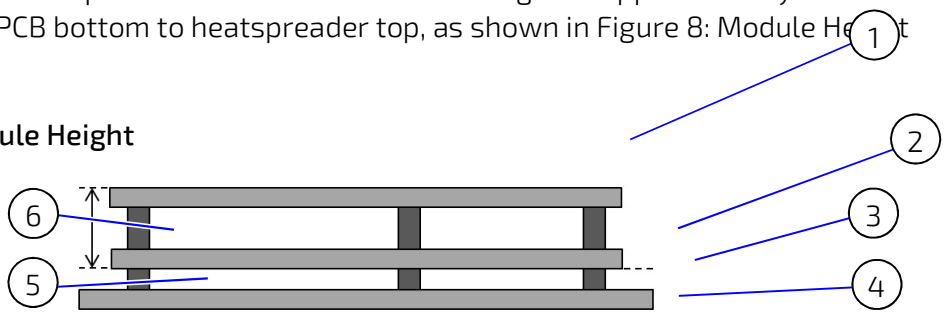
CAD drawings are available at EMD Customer Section.

8.1.1. Height

The height of the module depends on the height of the implemented cooling solution. The height of the cooling solution is not specified in the COM Express® specification.

The COM Express® specification defines a module height of approximately 13 mm from module PCB bottom to heatspreader top, as shown in Figure 8: Module Height below.

Figure 8: Module Height



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

8.2. Thermal Management, Heatspreader and Cooling Solutions

A heatspreader plate assembly is available from Kontron for the COMe-bEP7. The heatspreader plate on top of this assembly is NOT a heat sink. It works as a COM Express®-standard thermal interface to use with a heat sink or external cooling devices.

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

60°C for commercial grade modules

85°C for industrial temperature grade modules (E2)

You can use many thermal-management solutions with the heatspreader plates, including active and passive approaches.

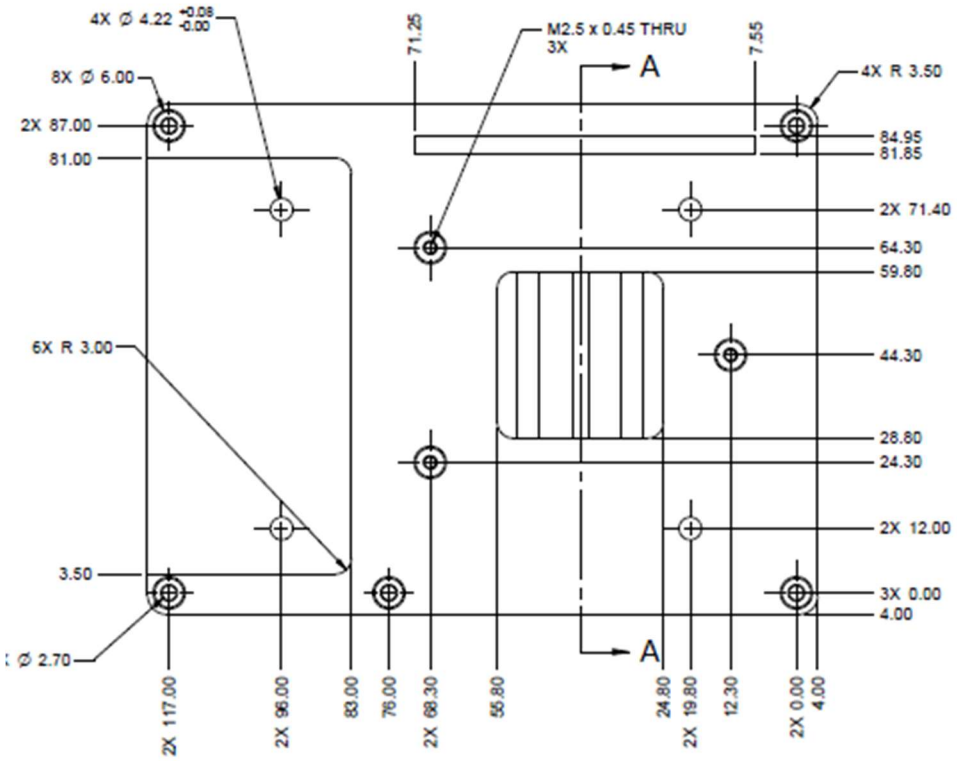
The optimum cooling solution varies, depending on the COM Express® application and environmental conditions. Active or passive cooling solutions provided from Kontron for the COMe-bEP7 are usually designed to cover the power and thermal dissipation for a commercial grade temperature range used in a housing with proper air flow.

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

8.2.1. Heatspreader Dimensions

The following figure shows the heatspreader's dimensions and location on the module.

Figure 9: Heatspreader Location and Dimensions



*All dimensions shown in mm.

9/ Features and Interfaces

9.1. SPI boot

The COMe-bEP7 supports boot from an external SPI Flash. It can be configured by pin A34 (BIOS_DIS0#) and pin B88 (BIOS_DIS1#) in following configuration:

Table 19: SPI Boot Pin Configuration

Configuration	BIOS_DIS0#	BIOS_DIS1#	Function
1	open	open	Boot on module BIOS
2	GND	open	Not supported
3	open	GND	Boot on carrier SPI
4	GND	GND	Boot on module SPI

By default, only the primary SPI Boot Device (chip select 0) is used in configuration 3 & 4. To access the secondary SPI device (chip select 1), the BIOS must be customized.

Table 20: Supported SPI boot flash types for 8-SOIC package

Size	Manufacturer	Part Number	Device ID
128 Mbit	Micron	MT25QU128ABA1E	0x20BA18
128 Mbit	Winbond	W25Q128JVSIG	0xEF7018

9.2. Updating SPI flash using AFU tool

To update the BIOS, you first need to boot in the EFI Shell or Linux OS with an USB key containing the AFU tool (for EFI Shell or Linux) and the binary to flash the SPI with, plugged on the system.

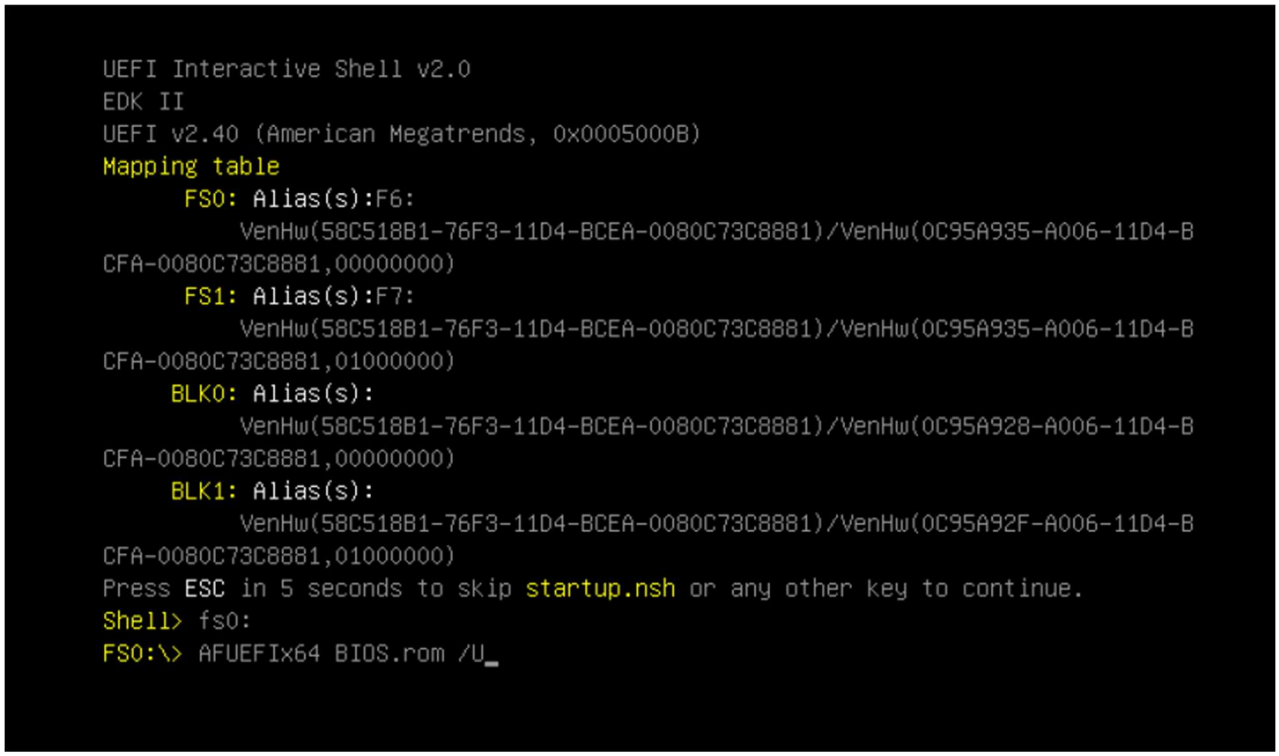
Note: with AFU, there is currently no support to boot from a SPI and program the "other" SPI by changing BIOS_DIS0#/BIOS_DIS1#. So, it cannot be used to program a blank part.

To update a SPI chip:

1. Connect a SPI flash with the correct size (similar to BIOS ROM file size) to the module SPI interface.
2. Turn on the system and boot in the EFI shell or Linux.

3. From the EFI shell, enter the name of the partition of your USB Key. In this example; write 'FS0:' then enter.

Figure 10: Entering USB Key Partition Name



   a. Alternatively, there is a Linux version AFU tool available to update the SPI (uses the same command line).

4. On your terminal, enter the following command:

   - Afu filename /b /p /n /k /l /x

5. When process is finished, power cycle the whole system.

6. Your system has now been updated.

For more information, visit the EMD Customer Section.

9.3. Triple Staged Watchdog Timer

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

The COMe-bEP7 offers a watchdog which works with three stages that can be programmed independently and used one by one.

Table 21: Time-out Events

0000b	No action	The stage is off and will be skipped.
0001b	Reset	A reset will restart the module and starts POST and operating system new.
0010b	NMI	A non-maskable interrupt (NMI) is a computer processor interrupt that cannot be ignored by standard interrupt masking techniques in the system. It is typically used to signal attention for non-recoverable hardware errors.
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 particular needs, contact Kontron customer 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 extended. (Only available in the first stage).
1000b	WDT Only	This setting triggers the WDT Pin on baseboard connector (COM Express® Pin B27) only.
1001b	Reset + WDT	
1010b	NMI + WDT	
1011b	SMI + WDT	
1100b	SCI + WDT	
1101b	DELAY + WDT -> No action*	

* After expiring the counter or triggering the stage action will be set to “No action”. The purpose is to allow a one-time delay before starting the actual time. WDT signal (mode 1101b) asserted after stage timeout, not after stage triggering.

9.4. WDT Signal

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

9.5. Power capping settings

Possibility to set a power level below actual CPU TDP. Refer to AMD EPYC processor specification.

Present options available in BIOS menu are:

1- Advanced -> AMD CBS -> NBIO Common Options -> cTDP Control
When set to [Auto], the fused maximum cTDP of the SoC is used.
When set to [Manual], can set customized cTDP value with option “cTDP”.
2- Advanced -> AMD CBS -> NBIO Common Options -> cTDP
Customized cTDP value (in Watts).

9.6. CPU Core Characteristics

The SP4/SP4r2 package is based on the AMD “Zen” CPU architecture.

9.6.1. Core P-States

The “Zen” core is designed to support as many as three performance states (P-states). P-state count, voltage, and frequency selection are defined by the specific processor model and optimized by voltage spread. The voltage for each P-state is optimized for maximum power savings between P-states at the highest frequency for that state.

9.6.2. Core C-States

C-states are processor core power states. C0 is the operational state in which instructions are executed, while higher numbered C-states (C1, C2, and so forth) are low-power states in which the core is idle. C-states are exposed through ACPI objects and can be dynamically requested by software.

The "Zen" core is designed to support as many as three AMD specified C-states: I/O-based C-states 0, 1, and 2.

9.6.2.1. Core C6 (CC6) State

The CPU is designed to support power gating in a C6 state. Power gating reduces the amount of power consumed by the core to further enhance energy efficiency. The CPU supports a core C6 mode (CC6).

9.6.3. Application Power Management (APM)

Application power management (APM) allows the processor to provide maximum performance while remaining within a specified power-delivery and thermal envelope. APM hardware dynamically monitors processor activity and generates an approximation of power consumption. If power consumption exceeds a defined power limit, a P-state limit is applied by APM hardware to reduce power consumption. APM ensures that average power consumption over a thermally significant time period remains at or below the defined power limit.

APM allows P-states to be defined with higher frequencies and voltages than could be used without APM. These P-states are referred to as boosted P-states.

The APM depends on the effective use of C-states and P-states. Disabling C-states greatly reduces the performance benefit of APM, as active cores would not be able to leverage the reduced power of idle cores.

APM can be disabled with the Advanced -> AMD CBS -> NBIO Common Options -> Core Performance Boost option.

9.7. SP4/SP4r2 Processor Power and Performance Optimization

The AMD SP4 and SP4r2 CPUs implement enhanced features that continuously monitor operational conditions (temperature, current, voltage, frequency, and power) and workload requirements to achieve maximum performance at minimal power consumption. These features are enabled by enhanced system design and optimal environment conditions, and work in combination to improve performance while maintaining baseline performance.

The default mode of operation remains Performance Deterministic, where the CPU deterministically perform at their lowest common denominator and implies energy consumed at rated TDP or less – this can be changed to Power Determinism, which forces the CPU to consume rated TDP and proportionally increases performance.

The Performance configuration can be set with the Advanced -> AMD CBS -> Zen Common Options -> Determinism Slider option.

9.8. ACPI Suspend Modes and Resume Events

The COMe-bEP7 supports the S-states S0, and S5.

The following events resume the system from S5:

Power Button
WakeOnLan

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

9.9. Fan Connector (J7)

Figure 11: 3-pin Fan Connector

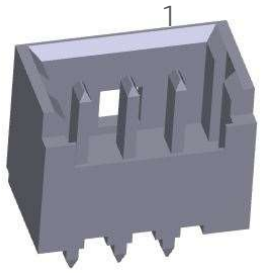


Table 22: 3-pin Fan Connector

Pin	Signal	Description	Type
1	TACHO	Rotation speed	I
2	PWM	PWM output	0-5 V
3	GND	Ground	PWR

Table 23: Signal Description

Signal	Description
GND	Power Supply GND signal
TACHO	Tacho input signal from the fan, for rotation speed supervision RPM (Rotations Per Minute).
PWM	Output signal for FAN speed control.

10/ System Resources

10.1. Interrupt Request (IRQ) Lines

Refer to your OS documentation on how to determine IRQ usage.

10.2. Memory Area

Refer to your OS documentation on how to determine memory usage.

10.3. I/O Address Map

The I/O-port addresses of the bEP7 are functionally identical to a standard PC/AT. All addresses not mentioned in this table should be available. We recommend that you do not use I/O addresses below 0100h with additional hardware for compatibility reasons, even if available.

Table 24: Designated I/O Port Addresses

I/O Address	Used for	Available	Comment
0000-001F	DMA Controller	No	Fixed
0020-002D	Interrupt Controller	No	Fixed
0002E-002F	Onboard UART	No	Fixed
0030-003D	Interrupt Controller	No	Fixed
0040-0042	Timer/Counter	No	Fixed
004E-004F	Winbond 83627DHG	No	When SIO present on carrier
0050-0052	Timer/Counter	No	Fixed

I/O Address	Used for	Available	Comment
0000-001F	DMA Controller	No	Fixed
0060-0064	Keyboard Controller	No	Fixed
0071-0077	RTC Controller	No	Fixed
0080	BIOS Post Code	No	Fixed
0081-0091	DMA Controller	No	Fixed
0092	Reset Generator	No	Fixed
0093-009F	DMA Controller	No	Fixed
00A0-00BD	Interrupt Controller	No	Fixed
00C0-00D1	DMA Controller	No	Fixed
00DE-00DF	DMA Controller	No	Fixed
00F0	FERR# / Interrupt Controller	No	Fixed
0240-0247	Winbond 83627DHG Serial Port 1	No	When SIO present on carrier
0248-024F	Winbond 83627DHG Serial Port 2	No	When SIO present on carrier
04D0-04D1	Interrupt Controller	No	Fixed

I/O Address	Used for	Available	Comment
0000-001F	DMA Controller	No	Fixed
0A80-0AFF	FPGA	No	Fixed
0CF9	Reset Generator	No	Fixed

Other I/O addresses are dynamically allocated for PCI devices and not listed here. Refer to your OS documentation on how to determine I/O addresses usage.

10.4. I2C Bus

Table 25: I2C Bus Port Addresses

8-bit Address	7-bit Address	Device	I2C Bus
		Embedded Controller FPGA	I2C_EXT
A0	50	COMe Module EEPROM	I2C_EXT
var.	var.	COMexpress connector	I2C_EXT
(AE)	(57)	(carrier EEPROM)	I2C_EXT

10.5. System Management (SM) Bus

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

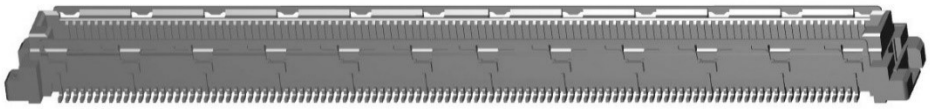
Table 26: Designated I/O Port Addresses

8-bit Address	7-bit Address	Device	Comment	SMBus
58h	0x2C	HWM NCT7802Y (non ECC Design)	Do not access directly under any circumstances.	SMB

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

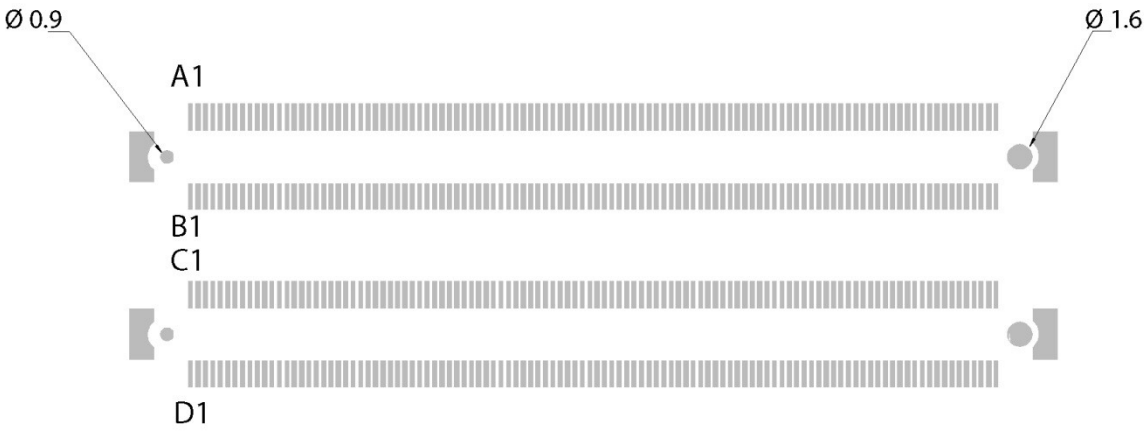
11/ COMe Connector Pin-out List

Figure 12: COMe Connector with 220 pins



This table lists the pins and signals according to the PICMG specification COM.0 Rev 3.0 Type 7 standard.

Figure 13: COMe Connector Pinout



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.

Table 27: Pin-out List

Pin	Row A	Row B	Row C	Row D
1	GND(FIXED)	GND(FIXED)	GND(FIXED)	GND(FIXED)
2	GBE0_MDI3-	GBE0_ACT#	GND	GND
3	GBE0_MDI3+	LPC_FRAME#/ ESPI_CS0#	USB_SSRX0 -	USB_SSTX0 -

Pin	Row A	Row B	Row C	Row D
4	GBE0_LINK100#	LPC_AD0/ESPI_IO_0	USB_SSRX0+	USB_SSTX0+
5	GBE0_LINK1000#	LPC_AD1/ESPI_IO_1	GND	GND
6	GBE0_MDI2-	LPC_AD2/ESPI_IO_2	USB_SSRX1-	USB_SSTX1-
7	GBE0_MDI2+	LPC_AD3/ESPI_IO_3	USB_SSRX1+	USB_SSTX1+
8	GBE0_LINK#	LPC_DRQ0#/ESPI_ALERT0#	GND	GND
9	GBE0_MDI1-	LPC_DRQ1#/ESPI_ALERT1#	USB_SSRX2-	USB_SSTX2-
10	GBE0_MDI1+	LPC_CLK/ESPI_CK	USB_SSRX2+	USB_SSTX2+
11	GND(FIXED)	GND(FIXED)	GND(FIXED)	GND(FIXED)
12	GBE0_MDI0-	PWRBTN#	USB_SSRX3-	USB_SSTX3-
13	GBE0_MDI0+	SMB_CK	USB_SSRX3+	USB_SSTX3+
14	GBE0_CTREF	SMB_DAT	GND	GND
15	SUS_S3#	SMB_ALERT#	10G_PHY_MDC_SCL3	10G_PHY_MDIO_SDA3
16	SATA0_TX+	SATA1_TX+	10G_PHY_MDC_SCL2	10G_PHY_MDIO_SDA2
17	SATA0_TX-	SATA1_TX-	10G_SDP2	10G_SDP3
18	SUS_S4#	SUS_STAT#/ESPI_RESET#	GND	GND
19	SATA0_RX+	SATA1_RX+	PCIE_RX6+	PCIE_TX6+
20	SATA0_RX-	SATA1_RX-	PCIE_RX6-	PCIE_TX6-
21	GND(FIXED)	GND(FIXED)	GND(FIXED)	GND(FIXED)

Pin	Row A	Row B	Row C	Row D
22	PCIE_TX15+	PCIE_RX15+	PCIE_RX7+	PCIE_TX7+
23	PCIE_TX15-	PCIE_RX15-	PCIE_RX7-	PCIE_TX7-
24	SUS_S5#	PWR_OK	10G_INT2	10G_INT3
25	PCIE_TX14+	PCIE_RX14+	GND	GND
26	PCIE_TX14-	PCIE_RX14-	10G_KR_RX3+	10G_KR_TX3+
27	BATLOW#	WDT	10G_KR_RX3-	10G_KR_TX3-
28	(S)ATA_ACT# (None on EPYC 3000)	GND(FIXED)	GND	GND
29	RSVD	RSVD	10G_KR_RX2+	10G_KR_TX2+
30	RSVD	RSVD	10G_KR_RX2-	10G_KR_TX2-
31	GND(FIXED)	GND(FIXED)	GND(FIXED)	GND(FIXED)
32	RSVD	SPKR(None on EPYC 3000)	10G_SFP_SDA3	10G_SFP_SCL3
33	RSVD	I2C_CK	10G_SFP_SDA2	10G_SFP_SCL2
34	BIOS_DIS0#/ ESPI_SAFS	I2C_DAT	10G_PHY_RST_23	10G_PHY_CAP_23
35	THRMTRIP#	THRM#	10G_PHY_RST_01	10G_PHY_CAP_01
36	PCIE_TX13+	PCIE_RX13+	10G_LED_SDA	RSVD
37	PCIE_TX13-	PCIE_RX13-	10G_LED_SCL	RSVD
38	GND	GND	10G_SFP_SDA1	10G_SFP_SCL1

Pin	Row A	Row B	Row C	Row D
39	PCIE_TX12+	PCIE_RX12+	10G_SFP_SDA0	10G_SFP_SCL0
40	PCIE_TX12-	PCIE_RX12-	10G_SDP0	10G_SDP1
41	GND(FIXED)	GND(FIXED)	GND(FIXED)	GND(FIXED)
42	USB2-	USB3-	10G_KR_RX1+	10G_KR_TX1+
43	USB2+	USB3+	10G_KR_RX1-	10G_KR_TX1-
44	USB_2_3_OC#	USB_0_1_OC#	GND	GND
45	USB0-	USB1-	10G_PHY_MDC_SCL1	10G_PHY_MDIO_SDA1
46	USB0+	USB1+	10G_PHY_MDC_SCL0	10G_PHY_MDIO_SDA0
47	VCC_RTC	ESPI_EN#	10G_INT0	10G_INT1
48	RSVD	USB0_HOST_PRSNT	GND	GND
49	GBE0_SDP	SYS_RESET#	10G_KR_RX0+	10G_KR_TX0+
50	LPC_SERIRQ/ESPI_CS1#	CB_RESET#	10G_KR_RX0-	10G_KR_TX0-
51	GND(FIXED)	GND(FIXED)	GND(FIXED)	GND(FIXED)
52	PCIE_TX5+	PCIE_RX5+	PCIE_RX16+	PCIE_TX16+
53	PCIE_TX5-	PCIE_RX5-	PCIE_RX16-	PCIE_TX16-
54	GPI0	GPO1	TYPE0#	RSVD
55	PCIE_TX4+	PCIE_RX4+	PCIE_RX17+	PCIE_TX17+
56	PCIE_TX4-	PCIE_RX4-	PCIE_RX17-	PCIE_TX17-
57	GND	GPO2	TYPE1#	TYPE2#

Pin	Row A	Row B	Row C	Row D
58	PCIE_TX3+	PCIE_RX3+	PCIE_RX18+	PCIE_TX18+
59	PCIE_TX3-	PCIE_RX3-	PCIE_RX18-	PCIE_TX18-
60	GND(FIXED)	GND(FIXED)	GND(FIXED)	GND(FIXED)
61	PCIE_TX2+	PCIE_RX2+	PCIE_RX19+	PCIE_TX19+
62	PCIE_TX2-	PCIE_RX2-	PCIE_RX19-	PCIE_TX19-
63	GPI1	GPO3	RSVD	RSVD
64	PCIE_TX1+	PCIE_RX1+	RSVD	RSVD
65	PCIE_TX1-	PCIE_RX1-	PCIE_RX20+	PCIE_TX20+
66	GND	WAKE0#	PCIE_RX20-	PCIE_TX20-
67	GPI2	WAKE1#	RAPID_SHUTDOWN	GND
68	PCIE_TX0+	PCIE_RX0+	PCIE_RX21+	PCIE_TX21+
69	PCIE_TX0-	PCIE_RX0-	PCIE_RX21-	PCIE_TX21-
70	GND(FIXED)	GND(FIXED)	GND(FIXED)	GND(FIXED)
71	PCIE_TX8+	PCIE_RX8+	PCIE_RX22+	PCIE_TX22+
72	PCIE_TX8-	PCIE_RX8-	PCIE_RX22-	PCIE_TX22-
73	GND	GND	GND	GND
74	PCIE_TX9+	PCIE_RX9+	PCIE_RX23+	PCIE_TX23+
75	PCIE_TX9-	PCIE_RX9-	PCIE_RX23-	PCIE_TX23-
76	GND	GND	GND	GND
77	PCIE_TX10+	PCIE_RX10+	RSVD	RSVD
78	PCIE_TX10-	PCIE_RX10-	PCIE_RX24+	PCIE_TX24+
79	GND	GND	PCIE_RX24-	PCIE_TX24-
80	GND(FIXED)	GND(FIXED)	GND(FIXED)	GND(FIXED)
81	PCIE_TX11+	PCIE_RX11+	PCIE_RX25+	PCIE_TX25+

Pin	Row A	Row B	Row C	Row D
82	PCIE_TX11-	PCIE_RX11-	PCIE_RX25-	PCIE_TX25-
83	GND	GND	RSVD	RSVD
84	NCSI_TX_EN	VCC_5V_SBY	GND	GND
85	GPI3	VCC_5V_SBY	PCIE_RX26+	PCIE_TX26+
86	RSVD	VCC_5V_SBY	PCIE_RX26-	PCIE_TX26-
87	RSVD	VCC_5V_SBY	GND	GND
88	PCIE_CK_REF+	BIOS_DIS1#	PCIE_RX27+	PCIE_TX27+
89	PCIE_CK_REF-	NCSI_RX_ER	PCIE_RX27-	PCIE_TX27-
90	GND(FIXED)	GND(FIXED)	GND(FIXED)	GND(FIXED)
91	SPI_POWER	NCSI_CLK_IN	PCIE_RX28+	PCIE_TX28+
92	SPI_MISO	NCSI_RXD1	PCIE_RX28-	PCIE_TX28-
93	GPO0	NCSI_RXD0	GND	GND
94	SPI_CLK	NCSI_CRS_DV	PCIE_RX29+	PCIE_TX29+
95	SPI_MOSI	NCSI_TXD1	PCIE_RX29-	PCIE_TX29-
96	TPM_PP	NCSI_TXD0	GND	GND
97	TYPE10#	SPI_CS#	RSVD	RSVD
98	SER0_TX	NCSI_ARB_IN	PCIE_RX30+	PCIE_TX30+
99	SER0_RX	NCSI_ARB_OUT	PCIE_RX30-	PCIE_TX30-
100	GND(FIXED)	GND(FIXED)	GND(FIXED)	GND(FIXED)
101	SER1_TX	FAN_PWMOUT	PCIE_RX31+	PCIE_TX31+
102	SER1_RX	FAN_TACHIN	PCIE_RX31-	PCIE_TX31-
103	LID#	SLEEP#	GND	GND
104	VCC_12V	VCC_12V	VCC_12V	VCC_12V

Pin	Row A	Row B	Row C	Row D
105	VCC_12V	VCC_12V	VCC_12V	VCC_12V
106	VCC_12V	VCC_12V	VCC_12V	VCC_12V
107	VCC_12V	VCC_12V	VCC_12V	VCC_12V
108	VCC_12V	VCC_12V	VCC_12V	VCC_12V
109	VCC_12V	VCC_12V	VCC_12V	VCC_12V
110	GND(FIXED)	GND(FIXED)	GND(FIXED)	GND(FIXED)

12/ uEFI BIOS

12.1. Starting the uEFI BIOS

The COMe-bEP7 uses a Kontron-customized, pre-installed and configured version AMI EFI BIOS Aptio ® V based on the Unified Extensible Firmware Interface (uEFI) specification and the Intel® Platform Innovation Framework for EFI. This uEFI BIOS provides a variety of new and enhanced functions specifically tailored to the hardware features of the COMe-bEP7.

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

The COMe-bEP7 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.

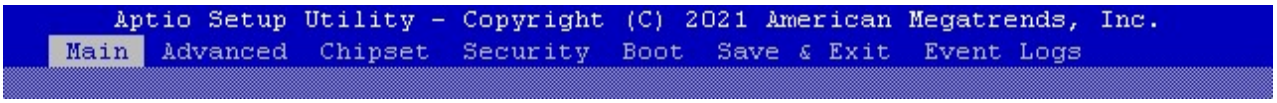
Table 28: Navigation Hot Keys Available in the Legend Bar

Sub-screen	Description
<→> 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
<RETURN>	<RETURN> key executes a command or selects a submenu
<->	<Minus> key selects the next lower value within a field
<+>	<Plus> key selects the next higher value within a field
<F1>	<F1> key invokes the General Help window
<F2>	<F2> key loads previous values
<F3>	<F3> key loads optimized defaults
<F4>	<F4> key Saves and Exits
<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
<K>	<K> key scrolls help area upwards.
<M>	<M> key scrolls help area downwards.

12.2. Setup Menus

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

Figure 14: Setup Menu Selection Bar



The Setup menus available for the COMe-bEP7 are:

Main
Advanced
Chipset
Security
Boot
Save & Exit
Event Logs

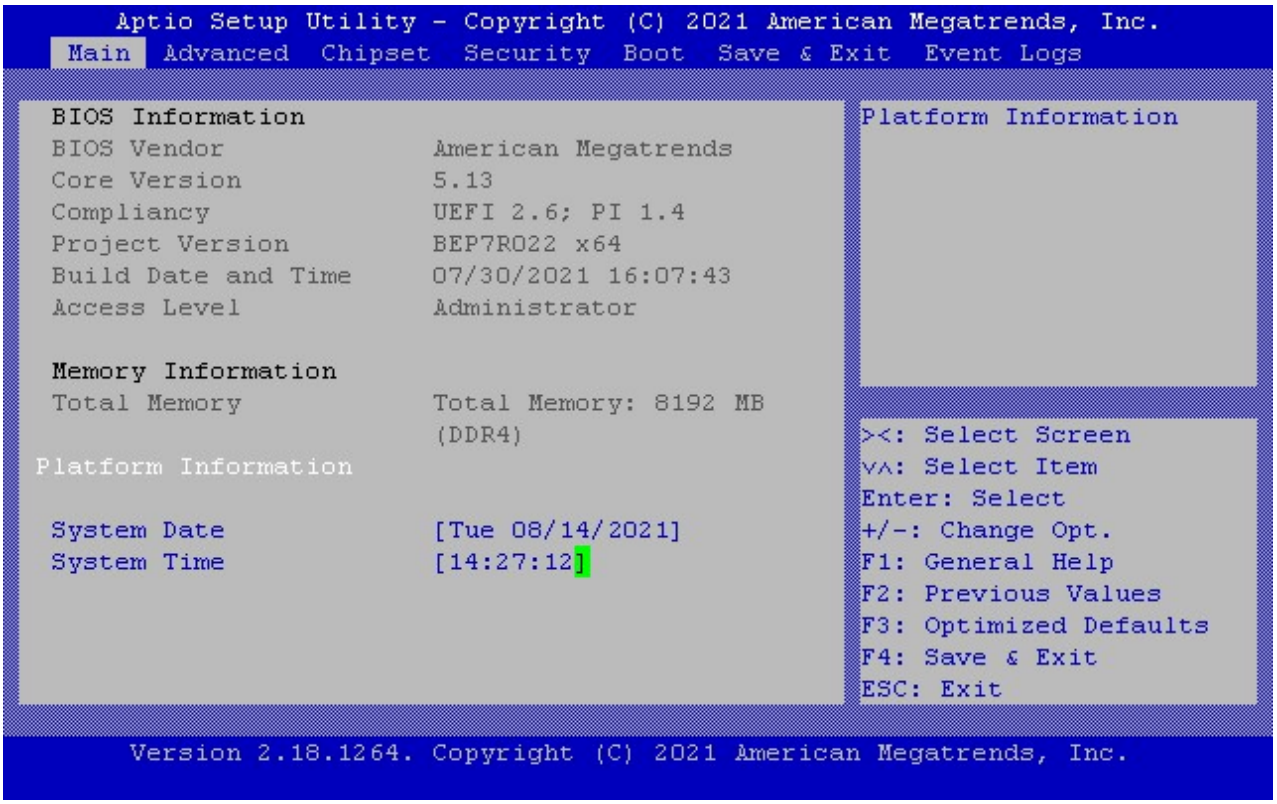
The currently active menu and the currently active uEFI BIOS Setup item are highlighted in white. Use the left and right arrow keys to select the Setup menus.

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.

12.3. Main Menu

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

Figure 15: Main Setup Menu



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

Table 29: Main Setup Menu Sub-screens

Sub-Screen	Description
BIOS Information>	Read only field BIOS Vendor, Core Version, Compliancy, Project Version, Build Date and Time, Access Level
Memory Information>	Read only field Total memory
Platform Information>	Read only fields Product Name, Revision, Configuration, Serial #, MAC Address, Boot Counter, CPLD Rev

Sub-Screen	Description
System Date>	Displays the system date [Week Day mm/dd/yyyy]
System Time>	Displays the system time [hh:mm:ss]

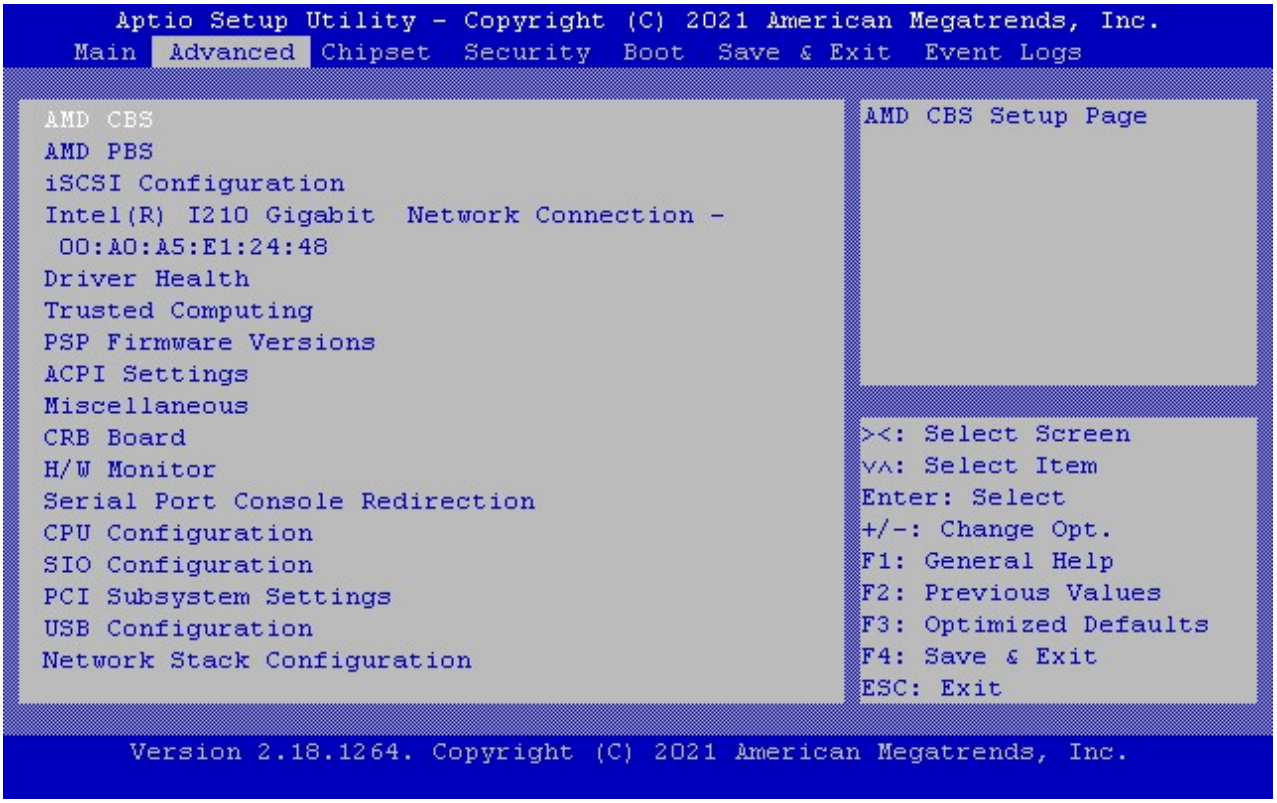
12.4. Advanced Setup Menu

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 16: Advanced Setup Menu



The following tables provides a description of the Advanced menu sub-screens and functions listed below and describes the content. Default settings are in **bold**. Some functions contain additional information.

12.4.1. AMD CBS Sub-Menu

Table 30: AMD CBS Sub-Screens

Sub-Screen	Second Level Sub-screen	Further Sub-Screens/Description	
Zen Common Options>	Core Performance Boost>	Disable CPB. [**Auto**, Disabled]	
	Global C-state Control>	Controls IO based C-state generation and DF C-states. [**Auto**, Enabled, Disabled]	
	Opcache Control>	Enables or disables the Opcache. [**Auto**, Enabled, Disabled]	
	Core/Thread Enablement >	Core/Thread Enablement	
		Disagree>	
		Agree>	
	NB Configuration>	IOMMU>	Enables or Disables IOMMU. [Disabled, Enabled, **Auto**]
		Concurrent Training>	Enables or Disables Concurrent Training. [Disabled, Enabled, **Auto**]
	NBIO Internal Poison Consumption>	Controls the NBIO Internal Poison Consumption. [Disabled, Enabled, **Auto**]	
	NBIO RAS Control>	Enables or disables the NBIO RAS Control. [Disabled, Enabled, **Auto**]	
	Determinism Slider>	Auto uses default performance determinism. [**Auto,** Power , Performance]	
	cTDP Control >	Auto uses the fused cTDP and Manual lets the users configure the cTDP. [Manual. **Auto**]	
	cTDP>	Only available when cTDP Control is set to Manual. [cTDP range available varies per CPU SKU]	

Sub-Screen	Second Level Sub-screen	Further Sub-Screens/Description	
NBIO Common Options> (continued)	PSI>	Disables PSI. [Disable, **Auto**]	
	ACS Enable>	Enables or disables the ACS. [Disabled, Enabled, **Auto**]	
	PICe ARI Support>	Enables Alternative Routing-ID Interpretation. [Disabled, Enabled, **Auto**]	
	CLDO_VDDP Control>	Manual lets the user configure the CLDO_VDDP Voltage. [Manual, **Auto**]	
	CLDO_VDDP Voltage>	The user must manually cold reset the system so that the CLDOs get re-latched otherwise the voltage change will not take effect. Only available when CLDO_VDDP Control is set to Manual. [0, 1, …]	
	HD Audio Enable>	Enables or disables HD Audio. [Disabled, Enabled, **Auto**]	
	Block PCIe Loopback>	Block PCIe Loopback mode for hot plug slots. [Disabled, Enabled, **Auto**]	
	CRS Delay>	CRS delay for hot plug ports. [**6**]	
	CRS Limit>	CRS limit for hot plug ports. [**262**]	
	Hot Plug flags>	Ignore sideband>	Disables sideband. [**Disabled**, Enabled, Auto]
		Disable L1 w/a>	Disables L1 w/a. [**Disabled**, Enabled, Auto]
		Disable BridgeDis>	No BridgeDis update based on sideband. [**Disabled**, Enabled, Auto]
		Toggle RRC Enable>	Toggle RRC Enable during hot plug events. [**Disabled**, Enabled, Auto]
		IRQ sets BridgeDis>	Register control of BridgeDis only follows DL_Active. [**Disabled**, Enabled, Auto]
		SATA Controller>	[Disabled, Enabled, **Auto**]

Sub-Screen	Second Level Sub-screen	Further Sub-Screens/Description		
FCH Common Options>	SATA Configuration Options>	SATA Mode>	Select OnChip SATA Type. [**AHCI**, AHCI as ID 0x7904, Auto, RAID]	
		Sata RAS Support>	[Disabled, Enabled, **Auto**]	
		Sata Disabled AHCI Prefetch Function>	Enables or disables SATA Disabled AHCI Prefetch Function. [Disabled, Enabled, **Auto**]	
		Aggressive SATA Device Sleep Port 0>	Enables or disables Aggressive SATA Device Sleep on port 0. [Disabled, Enabled, **Auto**]	
FCH Common Options> (continued)	SATA Configuration Options> (continued)	DevSleep0 Port Number>	DEVSLP port 0. [**0**, 1, …]	
		Aggressive SATA Device Sleep Port 1>	Enables or disables Aggressive SATA Device Sleep on port 1. [Disabled, Enabled, **Auto**]	
		DevSleep1 Port Number>	DEVSLP port 1. [**0**, 1, …]	
	USB Configuration Options>	XHCI controller enable>	Enables or disabled the XCHI. [Enabled, **Disabled**, Auto]	
			Additionnal information: This field needs to be enabled in order for the XHCI Port PHY fields to be displayed.	
		MCM USB enable>	XCHI Controller1 enable (Die1) >	Enables or disables USB1 controller. [Enabled, Disabled, **Auto**]
			XCHI Controller2 enable	Enables or disables USB2

Sub-Screen	Second Level Sub-screen	Further Sub-Screens/Description		
FCH Common Options> (continued)			(MCM1/Die0) >	controller. [Enabled, Disabled, **Auto**]
			XCHI Controller3 enable (MCM1/Die1) >	Enables or disables USB3 controller. [Enabled, Disabled, **Auto**]
	Ac Power Loss Options>	Ac Loss Control>	Select Ac Loss Control Method. [**Always Off**, Always On, Reserved, Previous]	
	XGBE Configuration Options>	AMD XGBE Controller X>	Enable or Disable Ethernet Controller X. [**Enabled,** Disabled]	
		Ethernet PHY>	This options allows to select external PHY type. BackPlane interface will not use any External PHY. [RJ45 Ports, **SFP+ Ports**, BackPlane]	
		Redriver Presence>	Option to select if a platform level Redriver is connected to the Processor PHY. [**Not used,** Present]	
		SideBand Interface>	Sideband signal path between each MAC port and the sideband pads. Mode/ Output Pads. [I2C/ MDIO 0 or 2, I2C/ MDIO 1 or 3, **I2C / SFP**,	

Sub-Screen	Second Level Sub-screen	Further Sub-Screens/Description	
FCH Common Options> (continued)	XGBE Configuration Options> (continued)		MDIO/ MDIO 0 or 2, MDIO/ MDIO 1 or 3, MDIO/ SFP]
		Connection Type>	Indicates additional information about the device connected to the processor's SERDES PHY. [Port not used, **SFP+ (I2C Sideband),** MDIO PHY, BackPlane (no sideband)]
		MDIO ID>	If external PHY connected using MDIO sideband interface, MDIO ID of the PHY. If MDIO is not used by this port, set this to 0. [**0** ...]
	Miscellaneous Options>	Boot Timer Enable>	Boot Timer enable. Enable: force PMx44 bit 27 = 1 Disable: force PMx44 bit 27 = 0 Auto: Force PMx44 bit 27 = PcdBootTimerEnable [**Auto**, Enabled, Disable]
NTB Common Options>	NTB Enable>	Controls the NTB. [**Auto**, Enabled]	
		Additional Information: This field must be set to Enabled in order to access the following fields.	
	NTB Location>	NTB Location. [**Auto**, Socket0-Die0, Socket0-Die1, Socket0-Die2, Socket0-Die3, Socket1-Die0, Socket1-Die1, Socket1-Die2, Socket1-Die3]	

Sub-Screen	Second Level Sub-screen	Further Sub-Screens/Description
	NTB active on PCIeCore>	NTB enable on PCIe Core. [**Auto**, Core0, Core1]
	NTB Mode>	Select NTM Mode (Core 0, Port 0). [**Auto**, NTB Disabled, NTB Primary, NTB Secondary, NTB Random]
	Link speed>	Select Link Sped for NTB Mode (Core 0, Port 0). [**Auto**, Max Speed, Gen 1, Gen 2, Gen 3]

12.4.2. AMD PBS Sub-Menu

Table 31: AMD PBS Sub-Screens

Sub-Screen	Description
General information: This menu is used to configure PCIe lanes available to the carrier board (PCIe0 to PCIe31), with the exception of the PCIe8 to PCIe15 lanes that are not available if CPU is SP4r2 (Single Die). In this section, x refer to a numeric value representing a PCIe lane. The PCIe lanes configuration needs to be set for the carrier's configuration.	
Link Width at PCIEx>	Number of PCIe lanes for Link starting at COMe PCIEx. [Disabled, x1, x2, x4, x8, 16x]
PCIEx – Link Speed>	Root Port PCIe Link Speed. [**Max Speed**, PCIe Gen1, PCIe Gen2]
	Additional information: AMD EPYC® Embedded 3000 max PCIe speed is Gen3

12.4.3. Configuration Sub-Menu

Table 32: Configuration Sub-Screens

Sub-Screen	Description
iSCSI Initiator Name>	Enter the worldwide unique name of iSCSI initiator. Only IQN format is accepted with a range from 4 to 223.

12.4.4. Intel (R) I210 Gigabit Network Connection

Table 33: Intel (R) I210 Gigabit Network Connection Sub-Screens

Sub-Screen	Second Level Sub-screen/Description	
Firware Image Properties>	Read only fields. Option ROM version, Unique NVM/EEPROM ID, NVM Version.	
NIC Configuration>	Configure the Network device port	
	Link Speed>	[**Auto Negotiated**, 10 Mbps Half, 10 Mbps Full, 100 Mbps Half, 100 Mbps Full]
	Wake On LAN>	Enables or disables power on of the system via LAN. [**Disabled**, Enabled]
Blink LED>	Identify the physical Network port by blinking the associated LED. (Range: 0 -15)	

	[0]
Read only fields. UEFI Driver, Adapter PBA, Device Name, Chip Type, PCI Device ID, PCI Address, Link status, MAC Address.	

12.4.5. Driver Health Sub-Menu

Table 34: Driver Health Sub-Screens

This table only displays information about the onboard Intel (R) I210 NIC driver's health. However, the menu could be changed dynamically according to PCIe device(s) present in the carrier.

Sub-Screen	Sub-Screen/Description	
Intel (R) PRO/1000 9,4,06 PCI-E>	Read only field. Provides Health Status for the drivers/controllers.	
	Controller c8389518 Child 0>	Read only field. Provides Health Status for the controller/driver.
	Intel (R) I210 Gigabit Network Connection>	

12.4.6. Trusted Computing Sub-Menu

Table 35: Trusted Computing Sub-Screens

Sub-Screen	Further Sub-Screens/Description
Security device Support>	Enables or disables BIOS support for security device. Operating System will not show security device. The TCG EFI protocol and INT1A interface are not available. [Enabled, **Disabled**]
	Additional information: The previous field current value is not affected by <F3> key loads optimized defaults. In order to see the following fields, the previous field needs to be set to **Enabled** and the changes must be saved.
Active PCR Banks>	Read only field [**SHA-1, SHA256**]
Available PCR Banks>	Read only field [**SHA-1, SHA256**]
SHA-1 PCR Bank>	SHA-1 PCR Bank [**Enabled,** Disabled]
SHA256 PCR Bank>	SHA256 PCR Bank

Sub-Screen	Further Sub-Screens/Description
	[Enabled, **Disabled**]
Pending Operation>	Schedules an operation for Security Device Note: Computer reboots on restart in order to change the state of the security device. [**None**, TPM Clear]
Platform Hierarchy>	Platform Hierarchy [**Enabled**, Disabled]
Storage Hierarchy>	Storage Hierarchy [**Enabled**, Disabled]
Endorsement Hierarchy>	Endorsement Hierarchy [**Enabled**, Disabled]
TPM2.0 UEFI Spec Version>	Selects TCG2 Spec Version support: TCG_1_2 -compatible mode for Win8/Win10 and TCG_2: supports TCG2 protocol and event format for Win10 or later. [TCG_1_2, **TCG_2**]
Physical Presence Spec Version>	Select to tell OS to support either PPI Spec 1.2 or 1.3 Note: Some HCK tests might not support 1.3. [1.2, **1.3**]
TPM 20 InterfaceType>	Read only field [**TIS**]

12.4.7. PSP Firmware Versions Sub-Menu

Table 36: PSP Firmware Versions Sub-Screens

Sub-Screen	Description
PSP Firmware Version>	Read only fields. PSP Directory Level 1, PSP Recovery BL Ver, SMU FW Version, ABL Version, APCB Version, APOB Version, APPB Version.
	Read only fields. PSP Directory Level 2, PSP Bootloader Version, SMU FW Version, ABL Version, APCB Version, APOB Version, APPB Version.

12.4.8. ACPI Settings Sub-Menu

Table 37: ACPI Settings Sub-Screens

Sub-Screen	Second Level Sub-screen/Description
Enable ACPI Auto Configuration>	Enables or disables ACPI auto configuration. If enabled, the system uses generic ACPI settings that may not fit the system best. [Enabled, **Disabled**]

12.4.9. Miscellaneous Sub-Menu

Table 38: Miscellaneous Sub-Screens

Sub-Screen	Second Level Sub-screen/Description	Further Sub-Screens/Description
Generic LPC Decode Ranges>	Generic LPC Decode Ranges>	Enables or disables the generic LPC decode range [Enabled, **Disabled**]
Watchdog>	Auto Reload>	Enables automatic reload of watchdog timers on timeout [Enabled, **Disabled**]
	Global Lock>	Enable sets all Watchdog registers (except for WD_KICK) to read only, until board is reset. [Enabled, **Disabled**]
	Stage 1 Mode>	Selects action for this Watchdog stage [**Disabled**, Reset, NMI, SCI, Delay, WDT Signal only]
I2C Speed>	Selects internal I2C bus speed between (1 kHz and 400 kHz) For a default system 200KHz is appropriate.	
Onboard I2C Mode>	Sets the I2C onbaord mode. [**Mulitmaster**/BusClear]	
Sleep Button Mode>	Shows or hides Sleep Button inside ACPI OS. Default setting is disabled. [Enabled, **Disabled**]	
LID Switch Mode>	Read only field Shows or hides Lid Switch Inside ACPI OS. [**Disabled,** Enabled]	
SMBus device ACPI mode>	Hides the SMBus device from OS if set to Hidden, otherwise the device is visible in OS. [**Normal,** Hidden]	
CPLD device ACPI mode>	Hides the CPLD device from OS if set to Hidden, otherwise the device is visible in OS. [**Normal,** Hidden]	
Control COMe GPIOS in BIOS>	Enables or disables GPIO control in BIOS. If set to Disabled, then the GPIOS are not touched by the BIOS. [**Disabled,** Enabled]	
GPIO IRQ #>	Sets the IRQnumber to trigger by the CPLD on GPIO events. [**Disabled,** IRQ 5, IRQ 6, IRQ 7, IRQ 10, IRQ 11, IRQ 12, IRQ 14, IRQ 15]	

Sub-Screen	Second Level Sub-screen/Description	Further Sub-Screens/Description
I2C IRQ #>	[**Disabled,** IRQ 5, IRQ 6, IRQ 7, IRQ 10, IRQ 11, IRQ 12, IRQ 14, IRQ 15]	
PWRBTN IRQ #>	[Disabled, **IRQ 5**, IRQ 6, IRQ 7, IRQ 10, IRQ 11, IRQ 12, IRQ 14, IRQ 15]	

12.4.10. H/W Monitor Sub-Menu

Table 39: H/W Monitor Sub-Screens

Sub-Screen	Second Level Sub-screen/Description
Read only field Hardware Monitor name	
CPU Temperature>	Read only field. Displays CPU die temperature in °C.
Module Temperature>	Read only field. Displays module temperature in °C.
CPU Fan – Fan Control>	Set fan control mode. 'Disable' will totally stop the fan. a. Disable - stops fan. b. Manual – manually sets the fan. c. Auto – Hardware monitor controls cooling, similar to ACPI based 'Active Cooling', without producing a software load to the system. [Disabled, Manual, **Auto**]
CPU Fan – Fan Pulse>	Displays number of pulses fan produces during 1 revolution. (Range: 1-4) [**2**]
CPU Fan – Fan Trip Point>	Displays temperature at which the fan accelerates. (Range: 20°C – 80°) [**50**]
CPU Fan – Trip Point Speed>	Displays Fan speed at trip point in %. Minimum value is 30 %. Fan always runs at 100 % at TJmax (-10°C). [**50**]
CPU Fan – Reference Temperature>	Determines temperature source used for automatic fan control [Module Temperature, **CPU Temperature**]
External Fan- Fan Control>	Set fan control mode. 'Disable' will totally stop the fan. a. Disable - stops fan. b. Manual – manually sets the fan.

Sub-Screen	Second Level Sub-screen/Description
	c. Auto – Hardware monitor controls cooling, similar to ACPI based 'Active Cooling', without producing a software load to the system. [Disable, Manual, **Auto**]
External Fan– Fan Pulse>	Displays number of pulse fan produces during 1 revolution (Range: 1-4) [**2**]
External Fan- Fan Trip point>	Displays temperature at which fan accelerates. (Range: 20°C to 80°C) [**50**]
External Fan- Trip Point Speed>	Displays Fan speed at trip point in %. Minimum value is 30% Fan always runs at 100% at TJmax (-10°C) [**50**]
External Fan Reference Temperature>	Determines temperature source used for automatic fan control [Module Temperature, **CPU Temperature**]
Additional information External Fan An external fan can be connected to baseboard. The external fan control lines are routed via the COMe connector.	
5.0 V Standby>	Read only field Displays standby voltage
Batt Volt. at COMe Pin>	Read only field Displays battery voltage at COMe pin
Widerange Vcc>	Read only field Displays wide range VCC

12.4.11. Serial Port Console Redirection Sub-Menu

Table 40: Serial Port Console Redirection Sub-Screens

Sub-Screen	Second Level Sub	Further Sub-Screens/Description
COM0 Console Redirection> or COM1 Console Redirection>	Enables or disables console redirection via COMe module's COM0 or COM1. [**Enabled**, Disabled]	
COM0 Console Redirection Settings>	The settings specify how the host computer and the remote computer (which the user is using) will exchange data. Both computers should have the same or compatible settings.	

Sub-Screen	Second Level Sub	Further Sub-Screens/Description
or COM1 Console Redirection Settings> COM0 Console Redirection Settings> or COM1 Console Redirection Settings> (continued)	Terminal Type>	Emulation: ANSI: Extended ASCII character set VT100: ASCII character set VT100+: Extend VT100 to support color, function keys etc. VT-UTF8: uses UTF8 encoding to map Unicode chars onto 1 or more bytes. [VT100, VT100+, VT-UTF8, **ANSI**]
	Bits per Second>	Selects the serial port transmission speed. The sped must be matched on the other side. Long or noisy lines may require lower speeds. [9600, 19200, 38400, 57600, **115200**]
	Data Bits>	Data Bits [7, **8**]
	Parity>	A parity bit can be sent with the data bits to detect transmission errors. Even: parity bit is 0 if the num of 1's in the data bits is even. Odd: parity bit is 0 if the num of 1's in the data bits is odd. Mark: parity bit is always 1. Space: Parity bit is always 0. Mark and Space Parity do not allow error detection. [**None** , Even, Odd, Mark, Space]
	Stop Bits>	Stop bits indicate the end of a serial data packet. (A start bit indicates the beginning). The standard setting is 1 stop bit. Communication with slow devices may require more than 1 stop bit. [**1**, 2]
	Flow Control>	Flow control can prevent data loss from buffer overflow. When sending data, if the receiving buffers are full, a 'stop' signal can be sent to stop the data flow. Once the buffers are empty, a 'start' signal can be sent to re-start the flow. Hardware flow control uses two wires to send start/stop signals. [**None**, hardware RTS/CTS]

Sub-Screen	Second Level Sub	Further Sub-Screens/Description
COM0 Console Redirection Settings> or COM1 Console Redirection Settings> (continued)	VT-UTF8 Combo Key Support>	Enables VT-UTF8 combination key support for ANSI/VT100 terminals [**Enabled**, Disabled]
	Recorder Mode>	If enabled, only text will be sent. This is to capture terminal data. [Enabled, **Disabled**]
	Resolution 100x31>	Enables or disables extended terminal resolution. [Enabled, **Disabled**]
	Putty Keypad>	Select function key and key pad on putty. [**VT100**, LINUX, XTERMR6, SCO, ESCN, VT400]
Legacy Console Redirection Settings>	Redirection COM Port>	Selects a COM port to display redirection of legacy OS and legacy OPROM messages [**COM0**, COM1]
	Resolution>	On legacy OS, the number of rows and columns supported. [**80x24**, 80x25]
	Redirect After POST>	When Bootloader is selected, then Legacy Console Redirection is disabled before booting to legacy OS. When Always Enable is selected, then Legacy Console Redirection is always Enabled. [**Always Enable**, Bootloader]
Serial Port for Out-of-Band Management/ Windows Emergency Management Services (EMS) - Console Redirection>	Console redirection [Enabled, **Disabled**]	
Console Redirection Settings>	The settings specify how the host computer and the remote computer (which the user is using) will exchange data. Both computers should have the same or compatible settings.	

Sub-Screen	Second Level Sub	Further Sub-Screens/Description
Console Redirection Settings> (continued)	Out-of-Band Mgmt Port>	Microsoft Windows Emergency Management Services (EMS) allows for remote management of a Windows Server OS through a serial port. [**COM0**, COM1]
	Terminal Type>	VT-UTF8 is the preferred terminal type for out-of-band management. The next best choice is VT100+ and then VT100. See above, in Console Redirection Settings page, for more Help with Terminal Type/Emulation. [VT100, VT100+, **VT-UTF8**, ANSI]
	Bits per second>	Selects serial port transmission speed. The speed must be matched on the other side. Long or noisy lines may require lower speeds. [9600, 19200, 57600, **115200**]
	Flow Control>	Flow control can prevent data loss from buffer overflow. When sending data, if the receiving buffers are full, a 'stop' signal can be sent to stop the data flow. Once the buffers are empty, a 'start' signal can be sent to re-start the flow. Hardware flow control uses two wires to send start/stop signals. [**None**, Hardware RTS/CTS, Software Xon/Xoff]
	Read only fields. Data bits, Parity, StopBits.	

12.4.12. CPU Configuration Sub-Menu

Table 41: CPU Configuration Sub-Screens

Sub-Screen	Second Level Sub-screen/Description
SVM Mode>	Enables or disables CPU Virtualization. [**Enabled**, Disabled]
SMEE>	Control Secure Memory Encryption Enable. [**Enabled**, Disabled]
Node 0 Information>	Read-only fields. Information about the node 0.

12.4.13. SIO Configuration Sub-Menu

Table 42: SIO Configuration Sub-Screens

Sub-Screen	Second Level Sub-screen /Description	Further Sub-Screens/Description
Read only field AMI SIO Driver Version		
Serial Port 0> Serial Port 0> (continued)	Use This Device>	Enables the user to change the device's resource settings. New setting will be reflected on this setup page after system restart. [**Enabled**, Disabled]
	Logical Device Settings Current>	Read only field IO=3F8h; IRQ=4
	Logical Device Settings: Possible>	Allows the user to change the device's resource settings. New settings are reflected on the Setup page after system restarts. [**Use Automatic Settings**, IO=3F8h; IRQ=4, IO=3F8h; IRQ=3,4,5,7,9,10,11,12, IO=2F8h; IRQ=3,4,5,7,9,10,11,12, IO=3E8h; IRQ=3,4,5,7,9,10,11,12, IO=2E8h; IRQ=3,4,5,7,9,10,11,12]
Read Only field WARNING: Disabling SIO Logical Devices may have unwanted side effects. PROCEED WITH CAUTION.		
Serial Port 1>	Use This Device>	Enables the user to change the device's resource settings. New setting will be reflected on this setup page after system restart. [**Enabled**, Disabled]
	Logical Device Settings Current>	Read only field IO=2F8h; IRQ=3
	Logical Device Settings: Possible>	Allows the user to change the device's resource settings. New settings are reflected on the Setup page after system restarts. [**Use Automatic Settings**, IO=2F8h; IRQ=3,

Sub-Screen	Second Level Sub-screen /Description	Further Sub-Screens/Description
		IO=3F8h; IRQ=3,4,5,7,9,10,11,1, IO=2F8h; IRQ=3,4,5,7,9,10,11,12, IO=3E8h; IRQ=3,4,5,7,9,10,11,12, IO=2E8h; IRQ=3,4,5,7,9,10,11,12]
Read only field WARNING: Disabling SIO Logical Devices may have unwanted side effects. PROCEED WITH CAUTION.		

12.4.14. PCI Subsystem Settings Sub-Menu

Table 43: PCI Subsystem Settings Sub-Screens

Sub-Screen	Second Level Sub-screen /Description
Read only field PCI Bus Driver version	
Above 4G Decoding>	Enables or disables decoding in Address Space above '4G' for 64 bit capable devices. Note: Only if system supports 64 bit PCI decoding. [**Enabled**, Disabled]
SR-IOV Support>	Enables or disables single root IO virtualization support If the system has SR-IOV capable PCIe devices. [Enabled, **Disabled**]

12.4.15. USB Configuration Sub-Menu

Table 44: USB Configuration Sub-Screens

Sub-Screen	Second Level Sub-screen/Description
Read only fields USB Configuration, UBS Module Version, USB Controllers, and USB devices	
Legacy USB Support>	Enables legacy USB support. Enable- Supports legacy USB Auto– disables legacy support, if no USB devices are connected Disable-keeps USB devices available only for EFI applications [**Enabled**, Disabled, Auto]
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>	Enables or disables USB mass storage driver support [**Enabled**, Disabled]
USB Transfer Time-out>	Displays timeout value for control, bulk and interrupt transfers [1 sec, 5 sec, 10 sec, **20 sec**]
Device Reset Time-out>	Displays USB mass storage device start unit command time-out [10 sec, **20 sec**, 30 sec, 40 sec]

Sub-Screen	Second Level Sub-screen/Description
Device Power-up Delay>	Maximum time the device will take before it properly reports itself to the Host Controller. 'Auto' uses default value: for a Root port it is 100 ms, for a Hub port the delay is taken from Hub descriptor. [**Auto**, Manual]
Device power-up delay in seconds>	Delay range is 1..40 seconds, in one second increments. Default: 5 seconds
	Additionnal information: Device Power-up Delay must be set to Manual in order for this field to be displayed.

12.4.16. Network Stack Configuration Sub-Menu

Table 45: Network Stack Configuration Sub-Screens

Sub-Screen	Second Level Sub-screen /Description
Network Stack>	Enables or disables the UEFI network stack. [Enabled, **Disabled**]
	Additionnal information: This field needs to be enabled in order for the rest of the fields to be displayed.
Ipv4 PXE Support>	Enable Ipv4 PXE Boot Support. If disabled IPV4 PXE boot option will not be created. [**Enabled**, Disabled]
Ipv4 HTTP Support>	Enables or disables IPv4 HHTP boot support. If disabled, IPv4 HTTP boot support will not be avbailable. [Enabled, **Disabled**]
Ipv6 PXE Support>	Enable Ipv6 PXE Boot Support. If disabled IPV6 PXE boot option will not be created. [Enabled, **Disabled**]
Ipv6 HTTP Support>	Enables or disables IPv6 HHTP boot support. If disabled, IPv6 HTTP boot support will not be avbailable. [Enabled, **Disabled**]
IP6 Configuration Policty>	Set IP6 Coonfiguration Policy [**Automatic**, Manual]
PXE boot wait time>	Wait time to press ESC key to abort the PXE boot. Default: 0

Sub-Screen	Second Level Sub-screen /Description
	[**0** … 5]
Media detect count>	Number of times presence of media will be checked. Default: 1 [**1** … 50]

12.4.17. CSM Configuration Sub-Menu

Table 46: CSM Configuration Sub-Screens

Sub-Screen	Second Level Sub-screen/Description
CSM Support>	Enables or disables CSM Support. [Enabled, **Disabled**]
	Additionnal information: This field needs to be enabled in order for the rest of the fields to be displayed.
Read Only field CSM module version.	
Gate A20 Active>	To allow for gateA20 to be disabled. UPON REQUEST: GA20 can be disabled using BIOS services ALWAYS: Does not allow disabling GA20 This option is useful when any RT code is executed above 1 MB. [**Upon Request**, Always]
INT19 Trap response>	BIOS reaction on INT19 traping by Option ROM: IMMEDIATE: executed the trap right away POSTPONED: executed the trap during legacy boot [**Immediate**, Postponed]
Boot Option Filter>	Controls the legacy/UEFI Roms priority [UEFI and Legacy, Legacy only, **UEFI only**]
Network>	Controls the execution of UEFI and legacy PXE OpROM [Do not launch, **UEFI**, Legacy] Note: AMD XGBE ports only support UEFI PXE.
Storage>	Controls the execution of UEFI and legacy OpROM [Do not launch, **UEFI,** Legacy]
Video>	Controls the execution of UEFI and legacy video OpROM [Do not launch**, UEFI**, Legacy]
Other PCI devices>	Determins OpROM execution policy for devices other than network storage or video.

Sub-Screen	Second Level Sub-screen/Description
	[Do not launch, **UEFI**, Legacy]

12.4.18. Debug Port Table Configuration Sub-Menu

Table 47: Debug Port Table Configuration Sub-Screens

Sub-Screen	Second Level Sub-screen/Description
Debug Port Table>	Debug Port Table. [Enabled, **Disabled**]
	Debug Port Table 2. [Enabled, **Disabled**]

12.4.19. NVMe Configuration Sub-Menu

Table 48: NVMe Configuration Sub-Screens

Sub-Screen
Read only field Acts as a message showing information about the NVMe (Non-Volatile memory PCIe) devices connected to the system (either on the module if populated or on the carrier).

12.4.20. SATA Configuration Sub-Menu

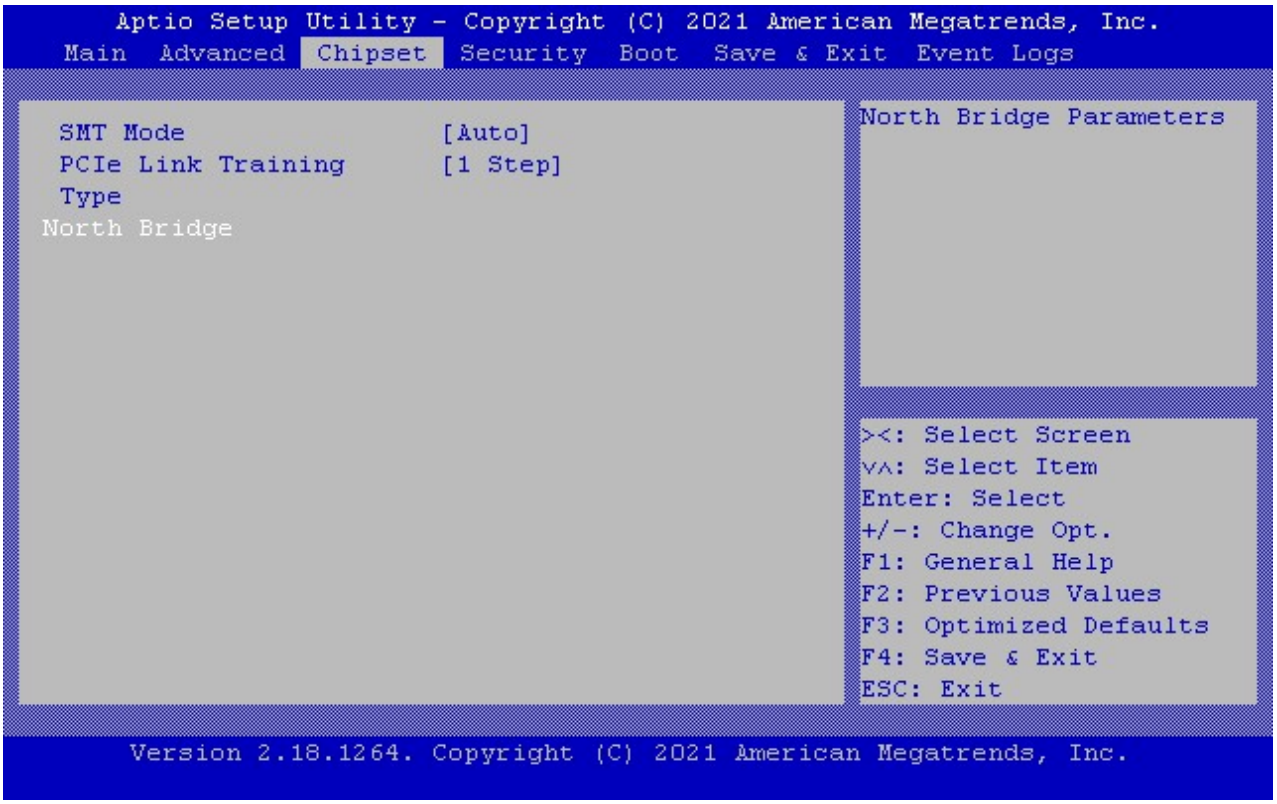
Table 49: SATA Configuration Sub-Screens

Sub-Screen
Read only field Acts as a message showing SATA ports status.

12.5. Chipset

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

Figure 17: Chipset Menu



The following table provides an over view of the Chipset menu sub-screens and functions listed below and describes the content. Default settings are in **bold**. Some functions contain additional information.

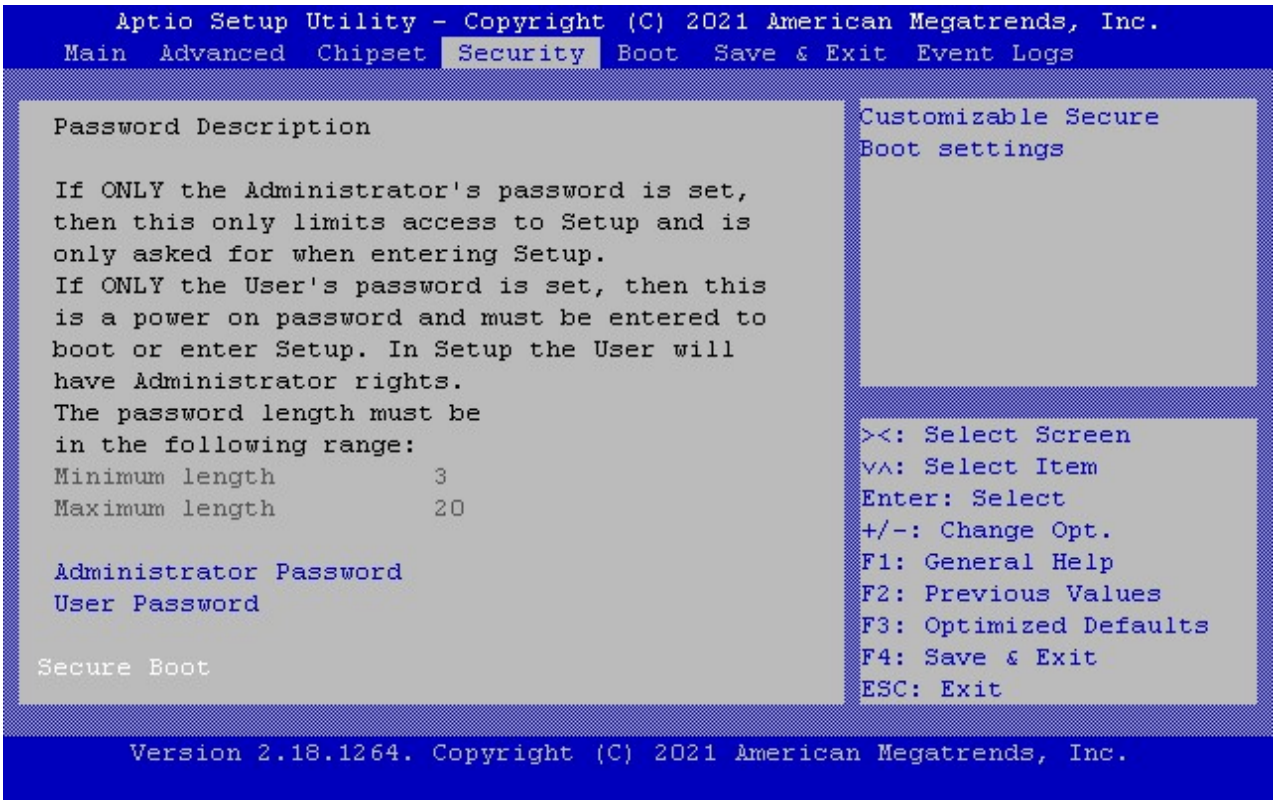
Table 50: Chipset Sub-screens and Functions

Sub-Screen	Second level Sub-Screen/Description
SMT Mode>	Simultaneous multithreading. Off = 1T single-thread. Auto=2T two-thread if capable. [Off, **Auto**]
PCIe Link Training Type>	PCIe Link training in 1 or 2 steps. [**1 Step**, 2 Step]
North Bridge>	North Bridge Configuration
	Read only fields. Memory Information, Total Memory.

12.6. Security Setup Menu

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

Figure 18: Security Setup Menu



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

Table 51: Security Setup Menu Functions

Function	Description
Administrator Password>	Set administrator password
User Password>	Set user password
Secure Boot Menu>	Read only field Shows the status of System mode, Secure boot and Vendor keys.

Function	Description		
Secure Boot Menu> (continued)	Attempt Secure Boot>	Secure boot is activated if : 1. System runs in user mode with enrolled Platform Key(PK) 2. CSM function is disabled. [Enabled, **Disabled**]	
	Secure Boot Mode>	Selects the secure boot mode. Customer mode enables users to change image execution policy and manage the secure boot keys. [Standard, **Custom**]	
	Key Management>	Provision Factory Defaults>	Install factory default Secure Boot Keys when system is in Setup Mode [Enabled, **Disabled**]
		Install Factory Default keys>	Forces system to user mode – install all factory default keys (PK, KEK, db, dbt, dbx. The change takes effect after reboot. [Yes, No]
		Enroll Efi Image>	Allow the image to run in Secure Boot Mode. Enroll SHA256 hash of the binary into Authorized Signature Database (db).
		Platform Key>	Enroll Factory Defaults or load the keys from a file with: 1. Public Key Certificate in: a. EFI_SIGNATURE_LIST b. EFI_CERT_X509 (DER encoded) c. EFI_CERT_RSA2048 (bin) d. EFI_CERT_SHA256 (bin) 2. Authenticated UEFI Variable Key source: Default, Custom, Mixed (*) modified from Setup menu
		Key Exchange Keys>	
		Authorized Signatures>	
		Forbidden Signatures>	
		Authorized Timestamps>	
		OsRecovery Signatures>	

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.

12.6.1. Remember the Password

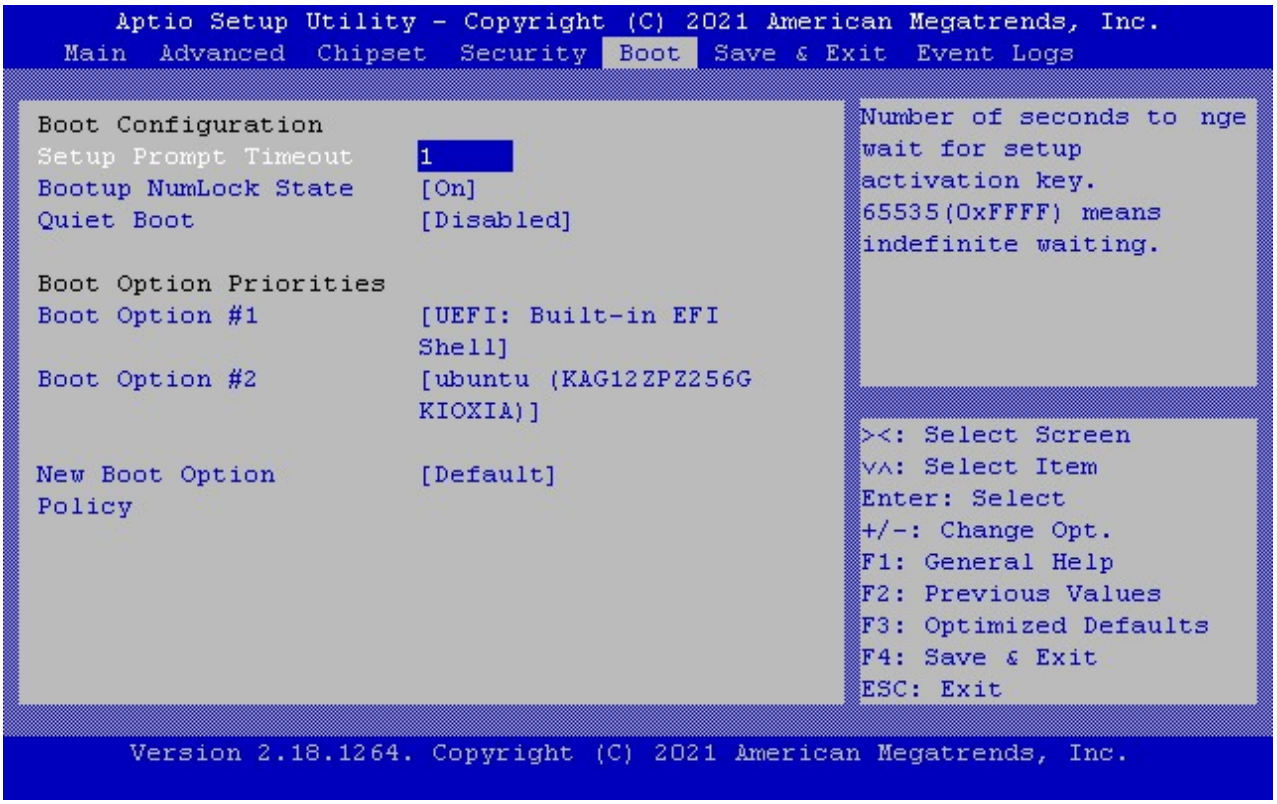
It is highly recommended to keep a record of all passwords in a safe place. Forgotten passwords result in the user being locked out of the system.

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.

12.7. Boot Setup Menu

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

Figure 19: Boot Setup Menu



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

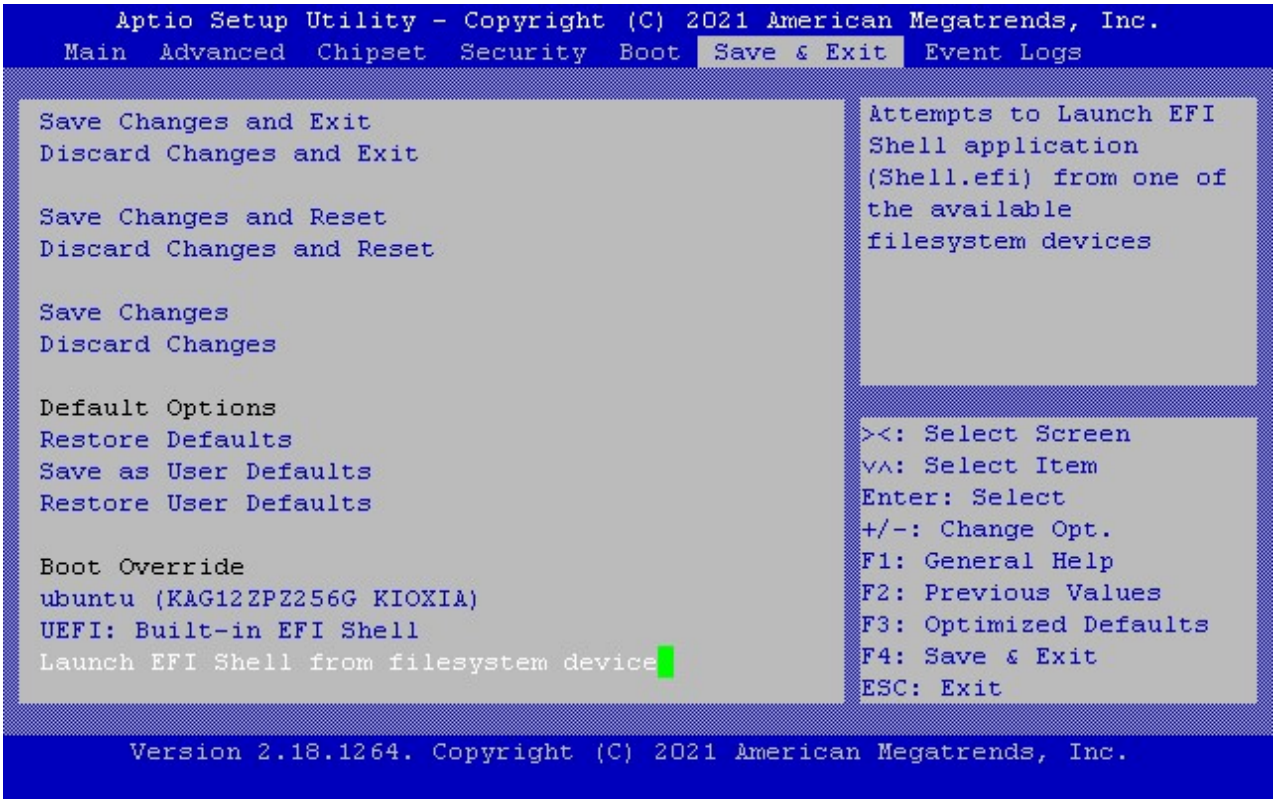
Table 52: Boot Setup Menu Functions

Function	Description
Setup Prompt Timeout>	Displays number of seconds to wait for the setup activation key. 65535(OXFFFF) means indefinite waiting [1]
Bootup NumLock State>	Selects keyboard NumLock state [**On**, Off]
Quiet Boot>	Enables or disables Quiet Boot [Enabled, **Disabled**]
Boot Option #X>	Sets the system boot order. This field could change according to the avalaible boot options. [**UEFI Built-in EFI shell** , Disabled]
	Additionnal information: When Enabling UEFI PXE support in BIOS (Advanced -> Network Stack Configuration), the Boot menu will only show "UEFI: AmdXgbe Network Driver x" device entries for the AMD 10 GBE ports that are connected to a server. This is a different behavior than what usually happens with Intel based Ethernet ports (always shown in Boot menu, even if they are not connected).
New Boot Option Policy>	Controls the placement of newly detected UEFI boot options. [**Default**, Place First, Place Last]

12.8. Save and Exit

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

Figure 20: Save and Exit Setup Menu



The following table shows Boot sub-screens and functions, and describes the content.

Table 53: Save and Exit Menu Functions

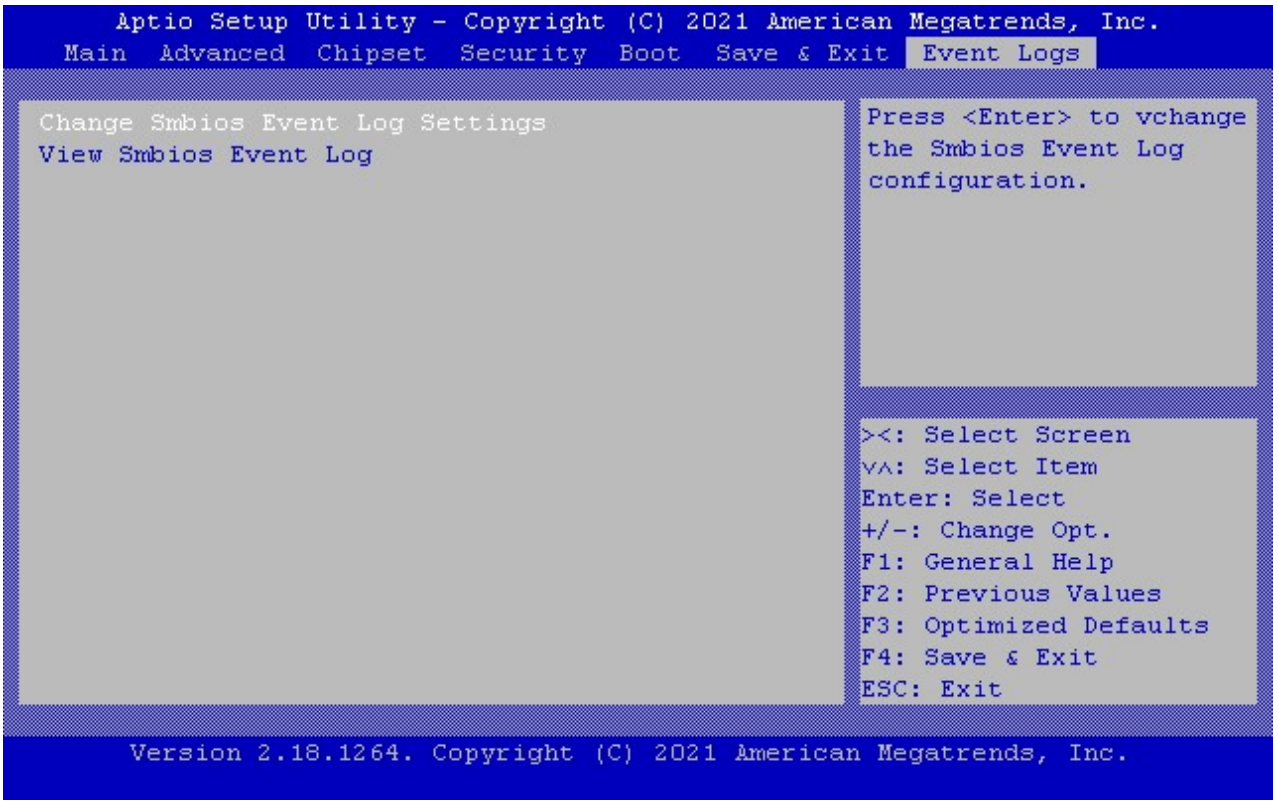
Function	Description
Save Options.	
Save Changes and Exit>	Exits system after saving changes
Discard Changes and Exit>	Exits system setup without saving changes
Save Changes and Reset>	Resets system after saving changes
Discard Changes and Reset>	Resets system setup without saving changes
Save Changes>	Saves changes made so far for any setup options
Discard Changes>	Discards changes made so far for any setup options
Default Options	
Restore Defaults>	Restores/loads standard default values for all setup options

Function	Description
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
Launch EFI Shell from filesystem device	Attempts to launch EFI Shell application (Shell.efi) from one of the available filesystem device.

12.9. Event Logs

The Event Logs Setup menu lists the event log settings and options.

Figure 21: Event Log Setup Menu



The following table shows Event Logs sub-screens and functions, and describes the content. Default settings are in bold and some functions include additional information

Table 54: Event Logs Setup Menu Functions

Function	Sub FunctionsDescription	
Change Smbios Event Log Settings>	Enabling and disabling options	
	Smbios Event Log>	Enables or disables all the Smbios event logging features during boot. [**Enabled**, Disabled]
	Erasing settings	
	Erase Event Log>	Choose option for erasing SmBIOS Event Log. Erasing is performed prior to any logging activation during reset. [**No**, Yes next reset , Yes every reset]
	When Log is Full>	Choose option for the reaction to a full Smbios Event log

Function	Sub FunctionsDescription	
Change Smbios Event Log Settings> (continued)		[**Do nothing**, Erase immediately]
	Smbios Event Log Standard Settings.	
	Log System Boot Event>	Enables or disables logging of the System boot event. [**Enabled**, Disabled]
	MECI>	Displays Multiple Event Count Increment value. The number of duplicate event occurrences that must pass before log entriy multiple event counter is updated. [**1**]
	METW>	Displays the Multiple Event Time Window value. The number of minutes that must pass between duplication log entries that utilize a multiple-event counter. (Range from 0-99 minutes) [**60**]
	Custom Options.	
	Log OEM Codes>	Enables or disables the logging of EFI staues codes as OEM codes if they have not already been converted to legacy. [**Enabled**, Disabled]
	Convert OEM Codes>	Enables or disables the converting of EFI status codes to standard Smbios types. Note: Not all may be translated. [Enabled, **Disabled**]
	Additional Information: All values changed here take effect only after the computer is restarted	
View SMbios Event Log>	Display all the SMbios Event Log.	

12.10. 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.

12.10.1. 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.

12.10.1.1. Entering the uEFI Shell

To enter the uEFI Shell, follow the steps below:

1. Power on the board.
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' script (if present), 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>
```

12.10.1.2. Exiting the uEFI Shell

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

1. Use the **exit** uEFI Shell command to boot the next device in the Boot menu, or return in BIOS Setup if no boot device detected.
2. Reset the board using the **reset** uEFI Shell command.

12.11. uEFI Shell Scripting

12.11.1. Startup Scripting

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

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

12.11.2. Create a Startup Script

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

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

12.12. Example of Startup Scripts

12.12.1. Execute Shell Script on other Harddrive

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

```
fs0:
bootme.nsh
```

12.13. Firmware Update

Firmware updates are typically delivered as a ZIP archive containing only the firmware images. The content of the archive with the directory structure must be copied onto a data storage device with FAT partition.
Refer to Chapter 9.2: Updating SPI Flash using AFU tool

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

13/ Technical Support

For technical support contact our Support department:

E-mail: support@kontron.com
Phone: +49-821-4086-888

Make sure you have the following information available when you call:

Product ID Number (PN),
Serial Number (SN)
Module's revision
Operating System and Kernel/Build version
Software modifications
Addition connected hardware/full description of hardware set up

The serial number can be found on the Type Label, located on the product's rear side.

Be ready to explain the nature of your problem to the service technician.

13.1. Warranty

Due to their limited service life, parts that by their nature are subject to a particularly high degree of wear (wearing parts) are excluded from the warranty beyond that provided by law. This applies to the CMOS battery, for example.

If there is a protection label on your product, then the warranty is lost if the product is opened.

13.2. Returning Defective Merchandise

All equipment returned to Kontron must have a Return of Material Authorization (RMA) number assigned exclusively by Kontron. Kontron cannot be held responsible for any loss or damage caused to the equipment received without an RMA number. The buyer accepts responsibility for all freight charges for the return of goods to Kontron's designated facility. Kontron will pay the return freight charges back to the buyer's location in the event that the equipment is repaired or replaced within the stipulated warranty period. Follow these steps before returning any product to Kontron.

1. Visit the RMA Information website:
http://www.kontron.com/support-and-services/support/rma-information

   Download the RMA Request sheet for **Kontron Europe GmbH** and fill out the form. Take care to include a short detailed description of the observed problem or failure and to include the product identification Information (Name of product, Product number and Serial number). If a delivery includes more than one product, fill out the above information in the RMA Request form for each product.

2. Send the completed RMA-Request form to the fax or email address given below at Kontron Europe GmbH. Kontron will provide an RMA-Number.

   Kontron Europe GmbH
   RMA Support
   Phone: +49 (0) 821 4086-0
   Fax: +49 (0) 821 4086 111
   Email: service@kontron.com

3. The goods for repair must be packed properly for shipping, considering shock and ESD protection.

Goods returned to Kontron Europe GmbH in non-proper packaging will be considered as customer caused faults and cannot be accepted as warranty repairs.

4. Include the RMA-Number with the shipping paperwork and send the product to the delivery address provided in the RMA form or received from Kontron RMA Support.

Appendix: Terminology

Term	Definition
ACPI	Advanced Configuration Power Interface – standard to implement power saving modes in PCAT systems
Basic Module	COM Express® 125mm x 95mm Module form factor.
AMD CBS	AMD Common BIOS Specification – AMD SoC related Setup options
AMD PBS	AMD PCIe BIOS Specification – PCIe configuration Setup options
BIOS	Basic Input Output System – firmware in PC-AT system that is used to initialize system components before handing control over to the operating system.
Carrier Board	An application specific circuit board that accepts a COM Express® Module.
AMD CBS	AMD Common BIOS Specification – AMD SoC related options
Compact Module	COM Express® 95x95 Module form factor
cTDP	Configurable TDP. BIOS option allowing boot time modification of TDP.
DIMM	Dual In-line Memory Module
DRAM	Dynamic Random Access Memory
EAPI	Embedded Application Programming Interface Software interface for COM Express® specific industrial functions System information Watchdog timer I2C Bus User storage area GPIO
EEPROM	Electrically Erasable Programmable Read-Only Memory
Extended Module	COM Express® 155mm x 110mm Module form factor.
Gb	Gigabit

Term	Definition
GBE	Gigabit Ethernet
GPI	General Purpose Input
GPIO	General Purpose Input Output
GPO	General Purpose Output
I2C	Inter Integrated Circuit – 2 wire (clock and data) signaling scheme allowing communication between integrated circuits, primarily used to read and load register values.
Legacy Device	Relicts from the PC-AT computer that are not in use in contemporary PC systems: primarily the ISA bus, UART-based serial ports, parallel printer ports, PS-2 keyboards, and mice. Definitions vary as to what constitutes a legacy device. Some definitions include IDE as a legacy device.
LAN	Local Area Network
LPC	Low Pin-Count Interface: a low speed interface used for peripheral circuits such as Super I/O controllers, which typically combine legacy-device support into a single IC.
LS	Least Significant
Mini Module	COM Express® 84x55mm Module form factor
MS	Most Significant
NA	Not Available
NC	No Connect
OEM	Original Equipment Manufacturer
PAL	Phase Alternating Line – video broadcast standard used in many European countries.
PATA	Parallel AT Attachment – parallel interface standard for hard-disk drives – also known as IDE, AT Attachment, and as ATA
PC-AT	“Personal Computer – Advanced Technology” – an IBM trademark term used to refer to Intel x86 based personal computers in the 1990s

Term	Definition
PCB	Printed Circuit Board
PCI	Peripheral Component Interface
PCI Express PCIE	Peripheral Component Interface Express – next-generation high speed Serialized I/O bus
PHY	Ethernet controller physical layer device
Pin-out Type	A reference to one of seven COM Express® definitions for the signals that appear on the COM Express® Module connector pins.
PS2 PS2 Keyboard PS2 Mouse	"Personal System 2" - an IBM trademark term used to refer to Intel x86 based personal computers in the 1990s. The term survives as a reference to the style of mouse and keyboard interface that were introduced with the PS2 system.
ROM	Read Only Memory – a legacy term – often the device referred to as a ROM can actually be written to, in a special mode. Such writable ROMs are sometimes called Flash ROMs. BIOS is stored in ROM or Flash ROM.
RTC	Real Time Clock – battery backed circuit in PC-AT systems that keeps system time and date as well as certain system setup parameters
SAS	Serial Attached SCSI – high speed serial version of SCSI
SCSI	Small Computer System Interface – an interface standard for high end disk drives and other computer peripherals
SoC	System on Chip
SPD	Serial Presence Detect – refers to serial EEPROM on DRAMs that has DRAM Module configuration information
SPI	Serial Peripheral Interface
SO-DIMM	Small Outline Dual In-line Memory Module
S0, S1, S2, S3, S4, S5	System states describing the power and activity level S0 Full power, all devices powered S1

Term	Definition
	S2 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: serial-interface standard for hard disks
SM Bus	System Management Bus
Super I/O	An integrated circuit, typically interfaced via the LPC bus that provides legacy PC I/O functions including PS2 keyboard and mouse ports, serial and parallel port(s) and a floppy interface.
TDP	Thermal Design Power
TPM	Trusted Platform Module, chip to enhance the security features of a computer system.
USB	Universal Serial Bus
VGA	Video Graphics Adapter – PC-AT graphics adapter standard defined by IBM.
WDT	Watch Dog Timer
XGBE	10 GbE

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

www.kontron.com