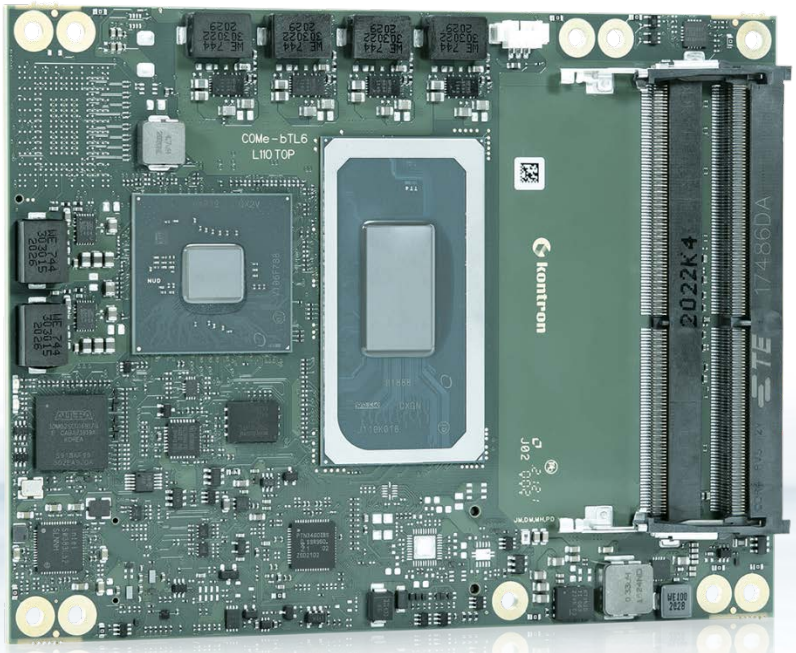
USER GUIDE



COMe-bTL6

User Guide. Rev. 2.2

Doc. ID: 1068 8679

This page has been intentionally left blank

COME-BTL6 – USER GUIDE

Disclaimer

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

Kontron Europe GmbH

Gutenbergstraße 2
85737 Ismaning
Germany
www.kontron.com

Intended Use

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

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

⚠CAUTION	**Handling and operation of the product is permitted only for trained personnel within a work place that is access controlled. Follow the "General Safety Instructions" supplied with the product.**
NOTICE	**You find the most recent version of the "General Safety Instructions" online in the download area of this product.**
NOTICE	**This product is not suited for storage or operation in corrosive environments, in particular under exposure to sulfur and chlorine and their compounds. For information on how to harden electronics and mechanics against these stress conditions, contact Kontron Support.**

Revision History

Revision	Brief Description of Changes	Date of Issue	Author
1.0	Initial version	2022-Apr-08	CW
1.1	Ch. 2.3.3 Block Diagram and Ch. 2.3.12 PCIE Express Graphics (PEG) Gen 4 updated.	2022-May-03	CW
1.2	I2C pin numbering changed Ch 4.1 and added corrosive warning pg. 4.	2022-May-19	CW
1.3	Typo "PCIe configuration (8x1)" in chapter 2.3.11 corrected.	2022-May-24	hjs
1.4	Updated Table 4 Memory Accessories and Chapter 3.4 GPIO.	2022- July-19	CW
1.5	Update Ch. 5 COMe connector pin assignment tables.	2022-Aug-30	CW
1.6	Updated, Figure 1, HSIO signal names in Tables 11, 12, 14, and 16 and updated the the following in the pinout tables (PCIE_TX5+/-, PCIE_RX6+/-, PCIE_RX7+/-, PEG_LANE-Reversal and Rapid Shutdown.)	2022-Nov-07	CW
1.7	Updated support of non ECC/ECC in Table 2.	2022-Dec-12	CW
1.8	Update the cooling accessory information in Table 4	2022-Dec-22	CW
1.9	Updated description of Ethernet pins A4 and A5 and new logo	2023-Feb-15	CW
2.0	2.4.1.2 Voltage ripple changed to 200 mV and added the new logo.	2023-Aug-23	CW
2.1	PCIe GEN4 is supported on all available PEG Ports.	2023-Nov-20	CW
2.2	SPI boot flash device updated in Table 33.	2024-Jan-10	CW

Terms and Conditions

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

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

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

Customer Support

Find Kontron contacts by visiting Kontron Support: https://www.kontron.com/en/support-and-services.

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 https://www.kontron.com/en/support-and-services.

Customer Comments

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

Symbols

The following symbols may be used in this user guide

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

For Your Safety

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

High Voltage Safety Instructions

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

⚠CAUTION

Warning

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

⚠CAUTION

Electric Shock!

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

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

Special Handling and Unpacking Instruction

NOTICE

ESD Sensitive Device!

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

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

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

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

Lithium Battery Precautions

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

⚠CAUTION

Danger of explosion if the battery is replaced incorrectly.

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

General Instructions on Usage

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

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

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

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

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

Quality and Environmental Management

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

Disposal and Recycling

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

WEEE Compliance

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

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

Environmental protection is a high priority with Kontron.

Kontron follows the WEEE directive

You are encouraged to return our products for proper disposal.

Table of Contents

List of Tables

List of Figures

1/ Introduction

This user guide describes the COM Express® type 6 Computer-On-Module COMe-bTL6 made by Kontron and focuses on describing the module's special features. Kontron recommends users to study this user guide before powering on the module.

1.1. Product Description

The COMe-bTL6 is a basic form factor COM Express® type 6 Computer-On-Module designed for flexible implementation within multiple embedded industrial environments. The COMe-bTL6 is based on the Quad/Hexa/Octa 11th Generation Intel® Core™ technology and Xeon® W family of processors with integrated Graphics Processing Unit (GPU) within a BGA 1787 package and with a separate Series 500 mobile chipset.

Key features are:

- 11th Generation Intel® Core™ and Xeon® W series of processors
- Basic form-factor COM Express® Basic type 6 pinout, compatible with PICMG COM.0 Rev 3.0 spec
- Up to 64 GByte DDR4 memory (2x 32 GByte)
- High-speed connectivity: 8x PCI Express, 1x up to 2.5 Gb Ethernet, 4x USB 3.1 Gen 2 + 8x USB 2.0, 4x SATA Gen.3, 2x serial ports
- Up to four simultaneous displays 4K at 60 Hz
- Support for Industrial and commercial temperature grade environments

1.2. Product Naming Clarification

COM Express® defines a Computer-On-Module (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)
- Processor family identifier
  - TL
- Pinout type
  - Type 10
  - Type 7
  - Type 6
- Available temperature variants
  - Commercial
  - Extended (E1)
  - Industrial (E2)
  - Screened industrial (E2S)
- Processor Identifier
- Chipset identifier (if assembled)
- Memory size
- Memory module (#G)/eMMC pseudo SLC memory (#S)

1.3. COM Express® Documentation

The COM Express® specification defines the COM Express® module form factor, pinout and signals. For more COM Express® specification information, visit the PCI Industrial Computer Manufacturers Group (PICMG®) website.

1.4. COM Express® Functionality

All Kontron COM Express® basic modules contain two 220-pin connectors, each of which has two rows called row A & B on the primary connector and row C & D on the secondary connector. The COM Express® basic type 6 Computer-On-Module (COM) features the following maximum amount of interfaces according to the PICMG module pinout type.

Table 1: Type 6 and COM-bTL6 Functionality

Feature	Type 6	COM-bTL6
HD Audio	1x	1x
Gbit Ethernet	1x	1x up to 2.5 GbE
Serial ATA Gen3	4x	4x
PCI Express x 1	4x	8x PCIe 3.0
PCI Express x16 (PEG)	1x	1x 16 PCIe 4.0
USB Client	-	-
USB	4x USB 3.0/2.0 8x USB 2.0	4x USB 3.1 Gen 2 8x USB 2.0
VGA	1x	1x (option)
LVDS (eDP)	1x LVDS dual channel	LVDS dual channel 18/24 bit (default) or Up to 2x eDP (option)
DP++	3x	3x
SPI	1x	1x SPI/GSPI
LPC	1x	1x (pin shared with eSPI)
External SMB	1x	1x
External I2C	1x	1x
SDIO shared with GPIO	1x option	-
GPIO or SDIO	8x	8x GPIO (4x GPI/4x GPO)
UART (2-wire COM)	2x	2x UARTS (default: Chipset / option: Embedded Controller)
FAN PWM out	1x	1x

1.5. COM Express® Benefits

COM Express® defines a Computer-On-Module (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 module is based on the COM Express® specification. This standardization allows designers to create a single-system carrier board that can accept present and future COM Express® modules.

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

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

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

2/ Product Specification

The COM-bTL6 is available in different processor, memory and temperature variants to cover demands in performance, price and power. The following tables list the module variants for the temperature grades.

2.1. Module Variants

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

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

Part Number	Product Name	Description
38038-0000-45-8	COMe-bTL6 W-11865MLE RM590E	COM Express® basic pin-out type 6 Computer-on-Module with Intel® Xeon® W-11865MRE, 8x4.7 GHz, RM590E PCH, GT2, 2x DDR4 non-ECC/ECC SO-DIMM
38038-0000-47-7	COMe-bTL6 i7-i7-11850HE QM580E	COM Express® basic pin-out type 6 Computer-on-Module with Intel® Core™ i7-11850HE, 8x4.7 GHz, QM580E PCH, GT2, 2x DDR4 non-ECC SO-DIMM
38038-0000-44-6	COMe-bTL6 W-11555MLE RM590E	COM Express® basic pin-out type 6 Computer-on-Module with Intel® Xeon® W-11555MLE, 6x4.4 GHz, RM590E PCH, GT2, 2x DDR4 non-ECC/ECC SO-DIMM
38038-0000-46-5	COMe-bTL6 i5-11500HE QM580E	COM Express® basic pin-out type 6 Computer-on-Module with Intel® Core™ i5-11500HE, 6x4.6 GHz, QM580E PCH, GT2, 2x DDR4 non-ECC SO-DIMM
38038-0000-44-4	COMe-bTL6 i3-11100HE RM590E	COM Express® basic pin-out type 6 Computer-on-Module with Intel® Core™ i3-11100HE, 4x4.4 GHz, RM590E PCH, GT2, 2x DDR4 non-ECC SO-DIMM
38038-0000-44-3	COMe-bTL6 i3-11100HE QM580E	COM Express® basic pin-out type 6 Computer-on-Module with Intel® Core™ i3-11100HE, 4x4.4 GHz, QM580E PCH, GT2, 2x DDR4 non-ECC SO-DIMM
38038-0000-31-4	COMe-bTL6 W-11155MLE RM590E	COM Express® basic pin-out type 6 Computer-on-Module with Intel® Xeon® W-11155MLE, 4x4.4 GHz, RM590E PCH, GT2, 2x DDR4 non-ECC/ECC SO-DIMM
38038-0000-26-2	COMe-bTL6 Celeron 6600HE HM570E	COM Express® basic pin-out type 6 Computer-on-Module with Intel® Celeron® 6600HE, 2x2.6 GHz, HM570E PCH, GT2, 2x DDR4 non-ECC SO-DIMM

2.1.2. Extended temperature Grade Modules (E1, -25°C to 75°C)

Extended temperature grade modules (E1, -25°C to +75°C) are available as a standard product number, on request. Contact your local sales representative to find out more about available extended temperature variants.

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

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

Part Number	Product Name	Description
38039-0000-47-8	COMe-bTL6 E2 W-11865MRE RM590E	COM Express® basic pin-out type 6 Computer-on-Module with Intel® Xeon® W-11865MRE, 8x4.7GHz, RM590E PCH, GT2, 2x DDR4 non-ECC/ECC SO-DIMM
38039-0000-46-6	COMe-bTL6 E2 W-11555MRE RM590E	COM Express® basic pin-out type 6 Computer-on-Module with Intel® Xeon® W-11555MRE, 6x4.6 GHz, RM590E PCH, GT2, 2x DDR4 non-ECC/ECC SO-DIMM
38039-0000-44-4	COMe-bTL6 E2 W-11155MRE RM590E	COM Express® basic pin-out type 6 Computer-on-Module with Intel® Xeon® W-11155MRE, 4x4.4 GHz, RM590E PCH, GT2, 2x DDR4 non-ECC/ECC SO-DIMM

2.2. Accessories

Accessories are product specific, COMe-type 6 specific or general COMe accessories. For more information, contact your local Kontron Sales Representative or Kontron Inside Sales.

Table 4: Accessories

Part Number	Carrier	Description
38116-0000-00-5	COMe Eval Carrier2 T6	COM Express® Evaluation Carrier2 type 6 with 5 mm COMe connector
38115-0000-00-0	COMe Ref.Carrier–i T6 TMI	COM Express® Reference Carrier type 6 for industrial temperature

Part Number	Cooling	Description
38038-0000-99-0	HSP COMe-bTL6 CU-Core THREADED	Heatspreader for COMe-bTL6, Cu-core, threaded mounting holes
38038-0000-99-1	HSP COMe-bTL6 CU-Core THROUGH	Heatspreader for COMe-bTL6, Cu-core, through mounting holes
38025-0000-99-0C05	COMe Active Uni Cooler (w/o HSP)	Active Cooler for COMe-bxL6/bDV7 to be mounted on HSP
38025-0000-99-0C06	HSK COMe-Basic Passive (w/o HSP)	Passive Cooler for COMe-bxL6/bDV7 to be mounted on HSP

Part Number	Fan Cables	Description
96079-0000-00-0	KAB-HSP 200 mm	Cable adapter to connect fan to module (COMe Basis/Compact/Mini)
96079-0000-00-2	KAB-HSP 40 mm	Cable adapter to connect fan to module (COMe Basis/Compact/Mini)

Part Number	Memory	Description
97020-3232-BTL6	DDR4-3200 SODIMM 32 GByte	DDR4-3200, 32GB, 260P, 1600MHz, PC4-3200 SODIMM (0°C to +60°C)
97020-1632-BTL6	DDR4-3200 SODIMM 16 GByte	DDR4-3200, 16GB, 260P, 1600MHz, PC4-3200 SODIMM (0°C to +60°C)

Part Number	Memory	Description
97020-0832-BTL6	DDR4-3200 SODIMM 8 GByte	DDR4-3200, 8GB, 260P, 1600MHz, PC4-3200 SODIMM (0°C to +60°C)
97020-0432-BTL6	DDR4-3200 SODIMM 4 GByte	DDR4-3200, 4GB, 260P, 1600MHz, PC4-3200 SODIMM (0°C to +60°C)
97021-3232-BTL6	DDR4-3200 SODIMM 32 GByte	DDR4-3200, 32GB, E2, 260P, 1600MHz, PC4-3200 SODIMM, industrial temperature (-40°C to +85°C)
97021-1632-BTL6	DDR4-3200 SODIMM 16 GByte	DDR4-3200, 16GB,E2, 260P, 1600MHz, PC4-3200 SODIMM, industrial temperature (-40°C to +85°C)
97021-0832-BTL6	DDR4-3200 SODIMM 8 GByte	DDR4-3200, 8GB, E2, 260P, 1600MHz, PC4-3200 SODIMM, industrial temperature (-40°C to +85°C)
97021-0432-BTL6	DDR4-3200 SODIMM 4 GByte	DDR4-3200, 4GB, E2, 260P, 1600MHz, PC4-3200 SODIMM, industrial temperature (-40°C to +85°C)
97030-3232-BTL6	DDR4-3200 SODIMM 32 GByte ECC	DDR4-3200, 32GB, ECC, 260P, 1600MHz, PC4-3200 SODIMM (0°C to +60°C)
97030-1632-BTL6	DDR4-3200 SODIMM 16 GByte ECC	DDR4-3200, 16GB, ECC, 260P, 1600MHz, PC4-3200 SODIMM (0°C to +60°C)
97030-0832-BTL6	DDR4-3200 SODIMM 8 GByte ECC	DDR4-3200, 8GB, ECC, 260P, 1600MHz, PC4-3200 SODIMM (0°C to +60°C)
97030-0432-BTL6	DDR4-3200 SODIMM 4 GByte ECC	DDR4-3200, 4GB, ECC, 260P, 1600MHz, PC4-3200 SODIMM (0°C to +60°C)
97031-3232-BTL6	DDR4-3200 SODIMM 32 GByte ECC	DDR4-3200, 32GB, ECC, E2, 260P, 1600MHz, PC4-3200 SODIMM, industrial temperature (-40°C to +85°C)
97031-1632-BTL6	DDR4-3200 SODIMM 16 GByte ECC	DDR4-3200, 16GB, ECC, E2, 260P, 1600MHz, PC4-3200 SODIMM, industrial temperature (-40°C to +85°C)
97031-0832-BTL6	DDR4-3200 SODIMM 8 GByte ECC	DDR4-3200, 8GB, ECC, E2, 260P, 1600MHz, PC4-3200 SODIMM, industrial temperature (-40°C to +85°C)
97031-0432-BTL6	DDR4-3200 SODIMM 4 GByte ECC	DDR4-3200, 4GB, ECC, E2, 260P, 1600MHz, PC4-3200 SODIMM, industrial temperature (-40°C to +85°C)

2.3. Functional Specification

2.3.1. Technical Data

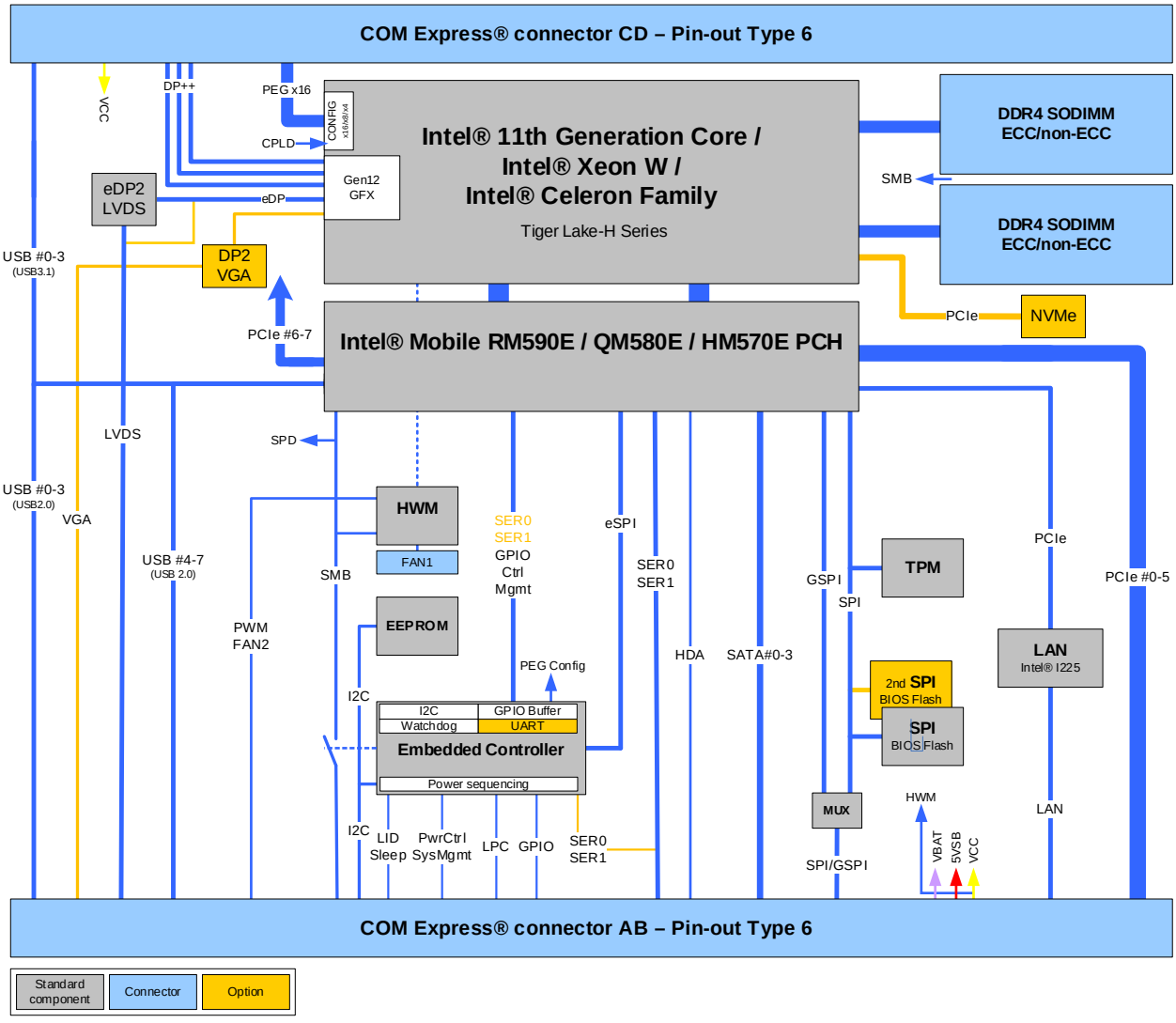
Table 5: Technical Data

Function	Definition
Compliance	COM Express® basic, pin-out type 6
Dimension (H X W)	125mm x 95 mm
Processors	Intel 11th generation processors: Core® i7-11850HE, i5-11500HE, i3-11100HE, Celeron® 6600HE Xeon® W-11865MLE, W-11555MLE, W-11155MLE, W-11865MRE, W-11555MRE, W-11155MRE
Chipset	Intel® Mobile HM570E Intel® Mobile QM580E Intel® Mobile RM590E
Main Memory	Up to 2x 32 GByte DDR4 SODIMM ECC or non ECC (total capacity 64 GByte) 3rd SODIMM socket on rear side (total capacity 96 GByte) (option)
Graphics Controller	Intel® Iris® Xe Graphics on i7/i5 processors Intel® UHD Graphics on i3/Celeron® processors
Displays	DDI1: DP++ DDI2: DP++ DDI3: DP++ VGA (option) LVDS dual channel 18/24bit (default) or up to 2x eDP (option)
Ethernet Controller	Intel® I225LM/I225IT
Ethernet	Up to 2.5 Gb Ethernet with TSN support (depends on processor)
Storage	4x SATA 6 Gb/s,
Flash On-board	Up to 1 TByte NVMe PCIe SSD NAND Flash (option)
PCI Express	8x PCIe 3.0 (8 GT/s) with default configuration 8x 1, optional config. 1x 4 + 4x 1, 2x4 PCI Express® for Graphics with default configuration 1 x16, optional config. 2x8, 1x8 + 2x4
USB	4x USB 3.1 Gen 2 8x USB 2.0
Serial	2x serial RX/TX ports from chipset (PCIe based, non-legacy, no RTS/CTS) (option: 2 UART serial RX/TX ports from Embedded Controller)
Audio	High Definition (HD) audio interface
Other Features	(G)SPI, LPC, SMB, Fast I²C, Staged Watchdog, RTC, Intel® Optane™ memory technology support via PCIe
Special Features	Trusted Platform Module (TPM) 2.0
Features on Request	vPRO (AMT/TXT/AES Support), eDP instead of LVDS, up to 3x PCIe x1 additional w/o Ethernet & SATA, NVMe SSD, Fail Save via 2nd SPI Flash
Power Management	ACPI 6.0
Power Supply	8.5 V – 20 V Wide Range, Single Supply Power
BIOS	AMI Aptio V
Operating Systems	Windows®10, Linux

Function	Definition
Temperature	Commercial temperature: 0 °C to +60 °C operating, -30 °C to +85 °C non-operating Extended temperature: -25 °C to +75 °C operating, -30 °C to +85 °C non-operating Industrial temperature: -40 °C to +85 °C operating, -40 °C to +85 °C non-operating
Humidity	93 % relative Humidity at 40 °C, non-condensing (according to IEC 60068-2-78)

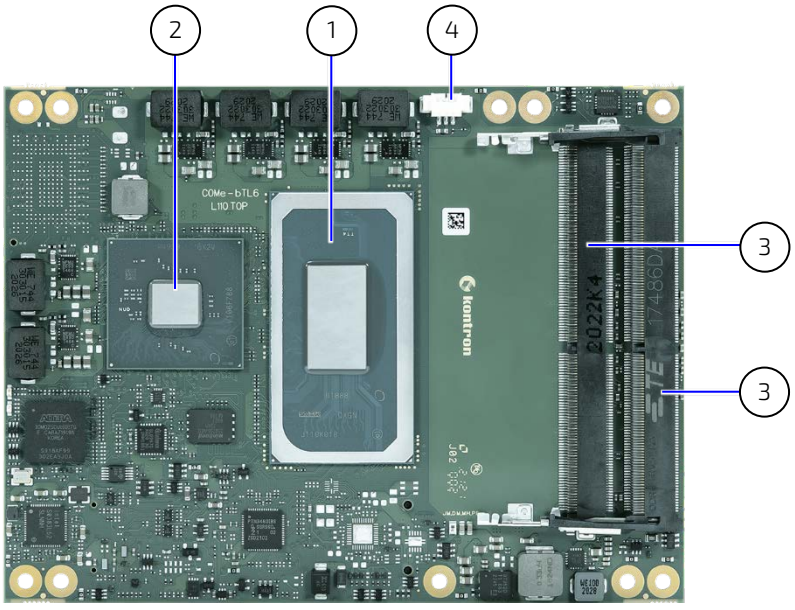
2.3.2. Block Diagram

Figure 1: Block Diagram COMe-bTL6



2.3.3. Front Side

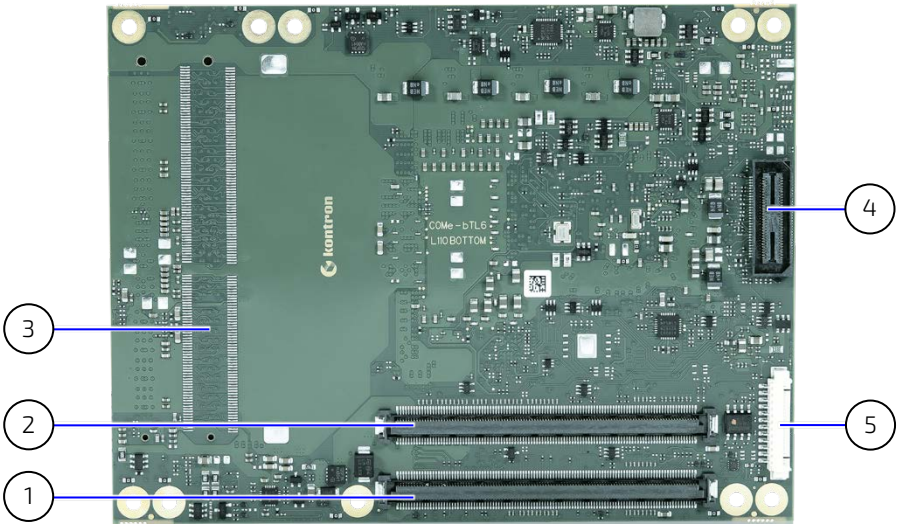
Figure 2: Front Side



1 Processor (CPU)
2 Chipset (PCH)
3 2x SODIMM memory sockets
4 3-pin fan connector

2.3.4. Rear Side

Figure 3: Rear Side



1 COMe interface connectors (X1A)
2 COMe interface connectors (X1B)
3 Space 3rd SODIMM memory socket (option)
4 XDP connector (option)
5 Programming connector for embedded controller

2.3.5. Processor (CPU)

The 11th Gen Intel® Core™, Celeron® and Xeon® W processor families support low latency for time sensitive application while running multiple applications on a single platform. This balance of performance and responsiveness makes the processors ideal for efficient management of real time multiply applications.

Key Benefits are:

- Up to eight cores and 16 threads CPU 11th Generation
- DDR4-3200 memory speeds
- Processor graphics Intel® UHD for 11th gen processors with up to 32 execution units and 4 supported displays
- Integrated PCIe 4.0 (PEG) lanes and PCIe 3.0 lanes
- Intel® Time Coordinated Computing Technology (Intel® TCC Technology) and Time- Sensitive Networking
- Intel® Deep Learning Boost for improved AI performance
- Intel® Thunderbolt™ 4
- Intel® Gaussian & Neural Accelerator,2.0
- Intel® Speed Shift Technology
- Intel® Turbo Boost Technology
- Intel vPro® Platform Eligibility
- Intel® Hyper-Threading Technology
- Intel® Virtualization Technology (VT-x) /
- Intel® Virtualization Technology for Directed I/O (VT-d)
- Intel® VT-x with Extended Page Tables (EPT)
- 64-bit Instruction Set

The following table lists the processor specifications for the COMe-bTL6 processor variants.

Table 6: 11th Generation Intel® Core™ Celeron® and Xeon® W Processor Spec

Processor	Core® i7-11850HE	Core® i5-11500HE	Core® i3-11100HE	Xeon® W-11865MLE	Xeon® W-11555MLE	Xeon® W-11155MLE	Celeron® 6600HE	Xeon® W-11865MRE	Xeon® W-11555MRE	Xeon® W-11155MRE
Use Condition	Commercial temperature[1] 0°C to 100°C							Industral embedded temperature[2] -40°C to 100°C		
# of Cores	8	6	4	8	6	4	2	8	6	4
Frequency Base/Turbo	2.6 GHz/ 4.2 GHz	2.6GHz/ 4.1 GHz	2.GHz/ 4.0 GHz	1.5 GHz/ 4.0 GHz	1.9 GHz/ 4.0 GHz	1.8 GHz/ 3.1 GHz	2.6 GHz	2.6 GHz/ 4.2 GHz	2.6 GHz/ 4.1 GHz	2.4 GHz/ 4.4 GHz
TDP (Up/Down)	45 W/ 35 W	45 W/ 35 W	45 W/ 35 W	25 W	25 W	25W	35W	45 W/ 35 W	45/ 35 W	45 W/ 35 W
Cache	24 MByte	12 MByte	8 MByte	24 MByte	12 MByte	8 MByte	8 MByte	24 MByte	12 MByte	8 MByte
TCC/TSN	no	no	no	no	no	no	no	yes	yes	yes
Intel® Graphics	UHD	UHD	UHD	UHD	UHD	UHD	UHD	UHD	UHD	UHD
Memory Support	DDR4-3200	DDR4-3200	DDR4-3200	DDR4-3200	DDR4-3200	DDR4-3200	DDR4-3200	DDR4-3200	DDR4-3200	DDR4-3200

[1] Within Tjunction limits the max. temperature range during operation is +-70°C, starting from boot time temperature

[2] Within Tjunction limits the max. temperature range during operation is +-90°C, starting from boot time temperature

The behavior is described in Intel document #608377 as DTR = Dynamic Temperature Range. For more information, contact Kontron Support

2.3.6. Chipset (PCH)

The COMe-bTL6 supports the Series 500 mobile chipset (Intel® Mobile HM570E, Intel® Mobile QM580E and Intel® Mobile RM590E). The chipset provides I/O support.

Table 7: Chipset (PCH)

I/O	USB 3.1 Gen 2/USB 2.0, PCIe Gen 3, SATA 3.0, Integrated LAN, 2.5 GbE TSN MAC[1]
Interfaces	SPI, eSPI, SMBus, HD Audio

[1] Option for processor variants Intel® Xeon® with RM590E PCH only, see Chapter 2.3.14: Ethernet LAN

2.3.7. System Memory

The COMe-bTL6 supports up to 64 GByte of SODIMM DDR4-3200 non-ECC/ECC memory or up to 96 GByte using a third SODIMM socket implemented in the bottom side of the module.

Table 8: System Memory

Socket	SODIMM DDR4-3200
Memory Type	DDR4-3200 1.2 V non-ECC/ECC
Channels	Dual-channel
Max Memory Module Size	Up to 64 GByte (2x 32 GByte) Up to 96 GByte (3x 32 GByte)
Memory Speed	3200 MTs (max.)

The two SODIMM memory sockets are located on the top side of the module where socket one is 4 mm height and socket two is 8 mm high. Each socket may be populated with a DDR4 SODIMM module mounted horizontally.

There is an option for a third SODIMM memory socket mounted horizontally on the bottom side of the module. Note: this increase in memory, decreases performance due to the asymmetric memory layout.

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

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

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

For a list of Kontron memory modules, see Table 4: Accessories

2.3.8. Graphics Interfaces

The COMe-bTL6 implements the processor graphics based the on Xe graphics core Architecture with substantial gains in performance and lower-power consumption over prior graphics generations. The Xe architecture supports up to 96 Execution Units (EUs) depending on the processor variant.

The modules supports up to four simultaneous displays 4K at 60 Hz or a single display 8k @ 60 Hz by joining two pipes over a single port.

If more than one active display port is connected, then the processor frequency may be lower than base frequency in thermally limited scenarios.

Table 9: Display Resolution

Display Interfaces Type	Maximum Resolution (Pixel)
eDP	4096 x 2304 @ 60 Hz
DP++	7680 x 4320 @ 60 Hz
LVDS	1920 x 1200
4K	Supported, @ 60 Hz
8K	Supported, @ 60 Hz

The module supports three DDI ports (DP++ /DP 1.4a ports), which cannot be overridden by other options. Additionally an eDP to LVDS bridge supports 18/24 Bit LVDS by default or the option without the eDP to LVDS bridge for up to two eDP ports by using the reduced signal bandwidth of eDP, when compared to LVDS, to support a second eDP. For legacy support a DP to VGA bridge support a VGA option. This VGA option does not prevent other port usage.

Table 10: Supported Display Types

COMe Port	CPU Port	Display Type	Description
DDI1	TCP0	DP++ (DP1.4a)	Standard on all product variants
DDI2	TCP1	DP++(DP1.4a)	Standard on all product variants
DDI3	TCP2	DP++(DP1.4a)	Standard on all product variants
LVDS (default)/ eDP1+eDP2 (option)	DDIA/ DDIA+DDIB	LVDS	eDP to dual channel LVDS (18/24 bit) with bridge chip
		eDP	Up to two eDP ports (eDP1 + eDP2) (Making use of eDP's smaller than LVDS signal bandwidth)
VGA (option)	TCP3	VGA	DP to VGA with bridge chip

Kontron strongly recommends the use of flat panels that support Extended Display Identification Data (EDID) or DisplayID.

Kontron recommends only using a DP-to-HDMI or DP-to-DVI passive adapter that is compliant to the DP Dual-Mode standard. If adapters are used with FET level shifter for DCC translation, display detection issues may occur.

To increase link margin, at 4K resolution a DP redriver on the carrier is recommended

2.3.9. HD Audio

The COMe-bTL6 supports audio using the processor's DDI (default) and carrier board audio using a HDA codec.

2.3.10. USB 3.1 Gen 2/USB 2.0

The COMe-bTL6 supports up to four USB 3.1 Gen 2 ports with 10 Gbit/s and up to eight USB 2.0 ports. Each USB 3.1 Gen 2 port is backwards compatible with USB 2.0. Therefore, the number of available USB 2.0 ports decreases with every used USB 3.1 Gen 2 port, with only four dedicated USB 2.0 ports. The modules supports four USB overcurrent signals.

Table 11: USB 3.1 Gen 2/USB 2.0 Port Configuration

COMe Connector	HSIO Lane #	USB Port	Description
USB_SS0	1	USB3_1/ USB2-1	USB 3.1 Gen 2 (10 Gb/s) or USB 2.0
USB_SS1	2	USB3-2/ USB2-2	USB 3.1 Gen 2 (10 Gb/s) or USB 2.0
USB_SS2	3	USB3-3/ USB2-3	USB 3.1 Gen 2 (10 Gb/s) or USB 2.0
USB_SS3	4	USB3-4/ USB2-4	USB 3.1 Gen 2 (10 Gb/s) or USB 2.0
USB4		USB2-5	USB 2.0 (dedicated)
USB5		USB2-6	USB 2.0 (dedicated)
USB6		USB2-7	USB 2.0 (dedicated)
USB7		USB2-8	USB 2.0 (dedicated)

Intel starts counting USB ports with 1, while the COMe Specification starts counting with 0.

2.3.11. General Purpose PCI Express 3.0

The COMe-bTL6 features up to eight PCIe Gen3 lanes [0-7] (8GT/s). The default configuration is 8x1 with the option for 1x4 + 4x1 and 2x4.

Table 12: General Purpose PCI Express 3.0 Lane Configurations

COMe Connector	HSIO Lane #	Supported Lane Configuration		
		8x1 (default)	1x4 + 4x 1	2x4
PCIe_0	11	x1	X4	x4
PCIe_1	12	x1		
PCIe_2	13	x1		
PCIe_3	14	x1		
PCIe_4	23	x1	x1	X4
PCIe_5	24	x1	x1	
PCIe_6	25	x1	x1	
PCIe_7	26	x1	x1	

To change the default PCIe configuration (8x1), a new BIOS version is required. For BIOS version information, see Kontron's Customer Section or contact Kontron Support.

2.3.12. PCI Express Graphics (PEG) Gen4

The COMe-bTL6 features PEG Gen4 lanes [0-16]. The default configuration is 1x 16.

The configurations 1x 8 + 2x 4 and 2x 8 can be set by the BIOS option: **Chipset> System Agent (SA) Configuration> PEG Width Configuration> PEG Width Configuration>**

Table 13: PCI Express Graphics (PEG) Lane Configurations

COMe Connector	Lane #	Supported Lane Configuration		
		1x 16 (default)	1x 8 + 2x 4	2x 8
PEG_0	1	x 16	x8	x8
PEG_1	2			
PEG_2	3			
PEG_3	4			
PEG_4	5			
PEG_5	6			
PEG_6	7			
PEG_7	8			
PEG_8	9		x4	x8
PEG_9	10			
PEG_10	11			
PEG_11	12			
PEG_12	13		x4	
PEG_13	14			
PEG_14	15			
PEG_15	16			

2.3.13. SATA 3.0

The COMe-bTL6 supports up to four SATA Generation 3 (6 Gb/s) lanes.

Table 14: SATA Port Connections

COMe Connector	HSIO Lane #	Description
SATA0	19	SATA Gen 3, 6 Gb/s
SATA1	20	SATA Gen 3, 6 Gb/s
SATA2	21	SATA Gen 3, 6 Gb/s
SATA3	22	SATA Gen 3, 6 Gb/s

2.3.14. Ethernet LAN

The COMe-bTL6 supports one 1 GbE/2.5 GbE Base-T Ethernet interface using the Intel® i225-LM Ethernet controller for commercial temperature grades and the Intel®I225-IT for industrial temperature grades (E2).

Modules variants with the Intel® Xeon® processor and RM590E PCH support an optional Ethernet port that implements SERDES signals directly to the COMe connector and supports TSN and WOL.

Table 15: Ethernet Port Connections

COMe Connector	HSIO Lane #	Description
2.5GBE w/TSN	15	2.5 GbE SERDES with TSN support and WOL (option)[1]
GBE0	18	1 GbE/2.5 GbE (on-module)

[1] Option for processor variants Intel® Xeon® with RM590E PCH only.

For 2.5 GbE Ethernet port speed, ensure the use of a compatible connector.

It is not recommended to use an integrated RJ45 connector module with the center tap shorted together with all the 4 pairs at the center-tap transformer. This increases the common mode noise and may create EMI. If this type of Integrated Connector module (ICM) is chosen, it is recommended to add in a discrete common choke in series to each PHY MDI differential line pairs.

2.3.15. COMe High-speed Interface Overview

The COMe-bTL6's 12 HSIO lanes support USB 3.1 Gen 2, SATA Gen 3, GBE/2.5GBE and PCIe Gen 3.0 (chipset PCH PCIe lanes).

Table 16: High-speed IO (HSIO) Lane Combinations

HSIO Lane #	High-Speed IO				
	USB 3.1 Gen 2	PCIe Gen 3.0	GbE	SATA 3.0	Description
1	USB_SS1				USB 3.1 Gen 2 (10 Gb/s)
2	USB_SS2				USB 3.1 Gen 2(10 Gb/s)
3	USB_SS3				USB 3.1 Gen 2 (10 Gb/s)
4	USB_SS4				USB 3.1 Gen 2 (10 Gb/s)
5					NC
6					NC
7					NC
8					NC
9					NC
10					NC
11		PCIe_0			PCIe 3.0 lane[2]
12		PCIe_1			PCIe 3.0 lane[2]
13		PCIe_2			PCIe 3.0 lane[2]
14		PCIe_3			PCIe 3.0 lane[2]
15			2.5GBE		2.5 GbE with TSN (SGMII) [1]
16					NC
17					NC
18			GBE0		10/100/1000/2500 Mbps GbE LAN (on-module)
19				SATA0	SATA Gen 3, 6 Gb/s
20				SATA1	SATA Gen 3, 6 Gb/s
21				SATA2	SATA Gen 3, 6 Gb/s
22				SATA3	SATA Gen 3, 6 Gb/s
23		PCIe_4			PCIe 3.0 lane[2]
24		PCIe_5			PCIe 3.0 lane[2]
25		PCIe_6			PCIe 3.0 lane[2]
26		PCIe_7			PCIe 3.0 lane[2]

[1] Option for processor variants Intel® Xeon® with RM590E PCH only.

[2] Chipset PCH PCIe lane

2.3.16. Storage

Table 17: Storage features:

Storage	Description
NVMe SSD	1x up to 1 TByte NVMe PCIe SSD NAND Flash (option)
Embedded EEPROM (Eeep)	1x Eeep 32kb (available on accessible I2C bus 8-bit address A0h)

2.3.17. BIOS/Software Features

Table 18: BIOS and Software Features

BIOS EFI	AMI UEFI (incl. support for AMI tools)
Software	Demo Utility for KEAPI usage for all supported OS BIOS/ EFI Flash Utility for EFI shell, Windows 10 and Linux BIOS/EFI Utility for users to implement Boot Logo and customized NVRAM (setup settings)
Operating Systems	Board Support Packages for: ▶ Windows 10 ▶ Linux (Yocto based)
Custom BIOS Settings/ Flash Backup	Supported

2.3.18. Additional Features

Table 19: General, Special Kontron and Optional Features

General Features	
Fast I2C	Connected to module EEPROM, carrier EEPROM and RTC clock
SPI	SPI external boot (GSPI option)
LID Signal	Supported
Sleep Signal	Supported
LPC	Used for external LPC on carrier board
RTC	Supported
SM Bus	Supported
SPI	Dedicated interface for TPM and flash memory
UART	2x seral RX/TX ports from chipset (PCIe based, non-legacy, no RTS/CTS) (option: 2 UART serial RX/TX ports from Embedded Controller)
Watchdog Support	Dual staged

Special Kontron Features	
Embedded API	KEAPI 3 for all Supported OS KEAPI packages are included in reference image
TPM 2.0	1x TPM 2.0 (hardware)

Optional Features (on request)	
eDP instead of LVDS	LVDS signals can be overlaid with eDP signal(s)
eSPI instead of LPC	eSPI from PCH for external SIO with additional

Optional Features (on request)	
NVMe SSD	Up to 1 TByte NVMe PCIe SSD NAND Flash
vPRO (AMT/TXT/AES)	Supported
Intel® Optane	From Intel® Mobile PCH
2nd SPI Flash	On-module fail-safe 2nd SPI flash implemented for additional safety
GSPI	General purpose SPI (in addition or instead of SPI external boot)

2.4. Electrical Specification

The module powers on by connecting to a carrier board via the COMe interface connector. Before connecting the module to the carrier board, ensure that the carrier board is switch off and disconnected from the main power supply at the time of connection. Failure to disconnect the main power supply from the carrier board could result in personal injury and damage to the module and/or carrier board. The COMe interface connector pins on the module limits the amount of power received.

⚠CAUTION

The module powers on by connecting to the carrier board using the interface connector. Before connecting the module's interface connector to the carrier board's corresponding connector, ensure that the carrier board is switch off and disconnected from the main power supply. Failure to disconnect the main power supply could result in personal injury and damage to the module and/or carrier board.

⚠CAUTION

Observe that only trained personnel aware of the associated dangers connect the module, within an access controlled ESD-safe workplace.

2.4.1. Power Supply Specification

The power specification of the module supports a supply voltage of 12 V (single power rail voltage) and a wide input voltage range of 8.5 V to 20 V. Other supported voltages are 5 V standby and 3.3 V RTC battery input.

Table 20: Electrical Specification

Supply Voltage (VCC) (range)	8.5 V to 20 V
Supply Voltage (VCC) (nominal)	12 V
Standby Voltage (VSB)	5 V ±5 % Note: 5V Standby voltage is not mandatory for operation
RTC Voltage (VBAT)	2.8 V to 3.47 V

⚠CAUTION

Only connect to an external power supply delivering the specified input rating and complying with the requirements of Safety Extra Low Voltage (SELV) and Limited Power Source (LPS) of UL/IEC 60950-1 or (PS2) of UL/IEC 62368-1.

NOTICE

To protect external power lines of peripheral devices, make sure that the wires have the right diameter to withstand the maximum available current and the enclosure of the peripheral device fulfils the fire-protection requirements of IEC/EN 62368-1.

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 must be measured individually for each case.

2.4.1.1. Power Supply Voltage Rise Time

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

2.4.1.2. Power Supply Voltage Ripple

The maximum power supply voltage ripple and noise is 200 mV peak-to-peak measured over a frequency bandwidth of 0 MHz to 20 MHz. The voltage ripple, must not cause the input voltage range to be exceeded.

2.4.1.3. Power Supply Inrush Current

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

2.4.2. Power Management

The Advanced Configuration and Power Interface (ACPI) 6.0 hardware specification supports features such as power button and suspend states. The power management options are available within the BIOS set up menu: **Advance>ACPI Settings>**

2.4.2.1. Suspend States

If power is removed, 5 V can be applied to the V_5V_STBY pins to support the ACPI suspend-states:

- Suspend to RAM (S3)
- Suspend-to-Disk (S4)
- Soft-off (S5)

If power is removed, the wake-up event (S0) requires 12 V VCC to power on the module for normal operation.

2.4.2.2. Power Supply Control Settings

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

Table 21: Power Supply Control Settings

COMe Signal	Pin	Description
Power Button (PWRBTN#)	B12	A PWRBTN# falling edge signal creates power button event (50 ms ≤ t < 4 s, typical 400 ms) at low level). Power button events can be used to bring a system out of S5 soft-off and other suspend states, as well as powering the system down. Pressing the power button for at least four seconds turns off power to the module Power Button Override
Power Good (PWR_OK)	B24	Indicates that all power supplies to the module are stable within specified ranges. PWR_OK signal goes active and module internal power supplies are enabled. PWR_OK can be driven low to prevent module from powering up until the carrier is ready and releases the signal. PWR_OK should not be deactivated after the module enters S0 unless there is a power fail condition.

COMe Signal	Pin	Description
Reset Button (SYS_RESET#)	B49	When the "SYS_RESET# "pin is detected active (falling edge triggered), it allows the processor to perform a "graceful" reset, by waiting up to 25 ms for the SMBus to enter the idle state before forcing a reset, even though activity is still occurring. Once reset is asserted, it remains asserted for 5 ms to 6 ms regardless of whether the SYS_RESET# input remains asserted or not.
Carrier Board Reset (CB_Reset#)	B50	When the "CB_Reset" from module to carrier is active low, the module outputs a request to the carrier board to reset.
SM-Bus Alert (SMB_ALERT#)	B15	When external battery manager is present and SMB_ALERT # connected, the module powers on even if the BIOS switch "After Power Fail" is set to "Stay Off".
Battery low (BATLOW#)	A27	BATLOW# indicates that the external battery is low and provides a battery-low signal to the module for orderly transitioning to power saving or power cut-off ACPI modes.
Wake Up Signal WAKE[0:1]	B66/ B67	Indicates PCIe wake up signal "Wake 0" or general purpose wake up signal "Wake 1"
Suspend Control (SUS_STAT#)	B18	SUS_STAT# indicates an imminent suspend operation. Used to notify LPC devices.

After a complete power loss (including battery voltage), there is an additional cold reset. This additional reset will not happen on any subsequent warm or cold reboots.

2.4.3. Power Supply Modes

The COM-bTL6 supports single power supply mode and ATX power supply mode. To change the power supply mode set the ATX and single power supply controls as described in the following sections.

2.4.3.1. ATX Power Supply Mode

To start the module in ATX mode, connect VCC and 5V Standby from a ATX PSU. As soon as the standby rail ramped up the PCH enters S5 state and starts the transition to S0. SUS_S3# (usually connected to PSU PS_ON#) turns on the main power rail (VCC). As soon as the PSU indicates that the power supply is stable (PWR_OK high) the PCH continues transition to S0. The input voltage must always be higher than 5V standby (VCC>5VSB) for modules supporting a wide input voltage range down to 8.5V.

The input voltage must always be higher than 5 V standby (VCC>5VSB) for modules supporting a wide input voltage range down to 8.5 V.

Table 22: ATX Mode Settings

State	PWRBTN#	PWR_OK	V5_Standby	PS_ON#	VCC
G3	x[1]	x[1]	0V	x[1]	0V
S5	high	low	5V	high	0V
S5 → S0	PWRBTN Event	low → high	5V	high →	0V→ VCC
S0	high	high	5V	low	VCC

[1] Defines that there is no difference if connected or open.

2.4.3.2. Single Power Supply Mode

To start the module in single power supply mode, connect VCC power and open PWR_OK at the high level. VCC can be 8.5 V to 20 V. To power on the module from S5 state, press the power button or reconnect VCC.

Suspend/Standby states are not supported in single power supply mode.

Table 23: Single Power Supply Mode Settings

State	PWRBTN#	PWR_OK	V5_Standby	VCC
G3	0V/x[1]	0V/x[1]	0V/x[1]	0V/x[1]
S5	high	open / high	open	VCC
S5 → S0	PWRBTN Event	open / high	open	reconnecting VCC
G3 → S0	high	open / high	open	connecting VCC

[1] Defines that there is no difference if connected or open.

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

2.5. Thermal Management

2.5.1. Heatspreader Plate Assembly

A heatspreader plate assembly is available from Kontron for the COMe-bTL6. The heatspreader plate assembly is NOT a heat sink. The heatspreader plate transfers heat as quickly as possible from the processor using a copper core positioned directly above the processor and a Thermal Interface Material (TIM). The heatspreader plate is factory prepared with a TIM screen printed on the contacts, see Figure 10, pos. 2 and 3 and may be fasten on the module without additional user actions.

The heatspreader plate works as a COM Express® standard thermal interface and must be used with a heat sink or external cooling devices 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 to the module's specification:

- 60°C for commercial temperature grade modules
- 75°C for extended temperature grade modules (E1)
- 85°C for industrial temperature grade modules by design (E2)

2.5.2. Active/Passive Cooling Solutions

Both active and passive thermal management approaches can be used with the heatspreader plate. The optimum cooling solution depends on the COM Express® application and environmental conditions. Kontron's active or passive cooling solutions are designed to cover the power and thermal dissipation for a commercial temperature range used in housing with a suitable airflow.

2.5.3. Operating with Kontron Heatspreader Plate (HSP) Assembly

The operating temperature requirements are:

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

Table 24: Heatspreader Temperature Specification

Temperature Grade	Requirements
Commercial Grade	at 60°C HSP temperature on MCP @ 100% load needs to run at nominal frequency
Extended Grade (E1)	at 75°C HSP temperature the MCP @ 75% load is allowed to start throttling for thermal protection
Industrial Grade (E2)	at 85°C HSP temperature the MCP @ 50% load is allowed to start throttling for thermal protection

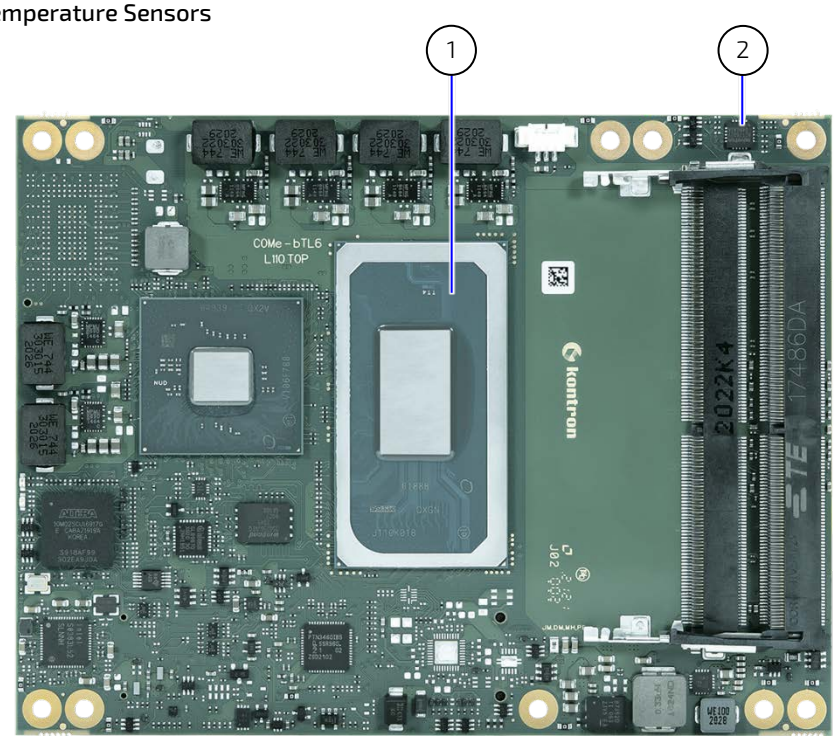
2.5.4. Operating without Kontron Heatspreader Plate (HSP) Assembly

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

2.5.5. Temperature Sensors

The module's processor is capable of reading its internal temperature. The on-module Hardware Monitor (HWM) chip uses an on-chip temperature sensor to measure the module's temperature close to the processor.

Figure 4: Module Temperature Sensors



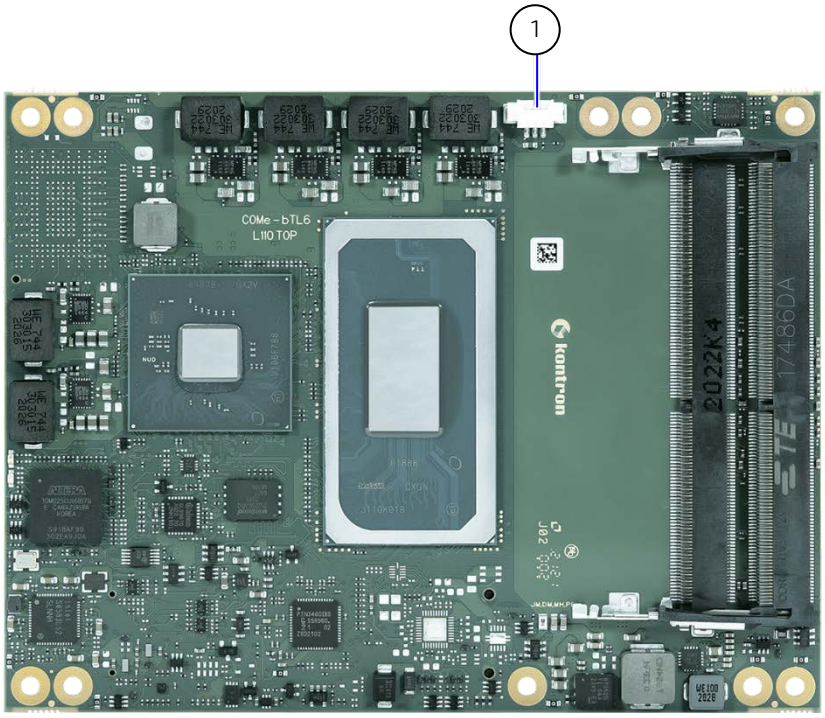
1 Processor (CPU)

2 Hardware Monitor

2.5.6. On-Module Fan Connector

The module's fan connector powers, controls and monitors an external fan. To connect a standard 3-pin connector fan to the module, use Kontron's fan cable, see Table 4: Accessories.

Figure 5: Fan Connector 3-Pin



1 3-pin fan connector

Table 25: Fan Connector (3-Pin) Pin Assignment

Pin	Signal	Description	Type
1	Fan_Tach_IN#	Fan input voltage from COMe connector	Input
2	V_FAN	12 V ±10% (max.) across module input range	PWR
3	GND	Power GND	PWR

If the input voltage is below or equal to 13 V, then the maximum supply current to the on-module fan connector is 350 mA. The maximum supply current is reduced to 150 mA if the input voltage to the module is between 13 V and 20 V.

NOTICE

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

2.6. Environmental Specification

The COMe-bTL6 variant support commercial and Industrial (E2) temperature grades with an option of extended temperatures grades. For temperature grade information, see Chapter 2.1 Module Variants.

Table 26: Environmental Specifications

Environmental		Description
Commercial Grade	Operating	0°C to +60°C (32°F to 140°F)
	Non-operating	-30°C to +85°C (.-22°F to 185°F)
Extended Grade (E1)	Operating	-25°C to +75°C (.-67°F to 185°F)
	Non-operating	-30°C to +85°C (-22°F to 185°F
Industrial Grade (E2)	Operating	-40°C to +85°C (-40°F to 185°F)
	Non-operating	-40°C to +85°C (-40°F to 185°F)
Relative Humidity (according to IEC 60068-2-78)		93 % @ 40°C, non-condensing
Shock (according to IEC / EN 60068-2-27)		Non-operating shock test (half-sinusoidal, 11 ms, 15 g)
Vibration (according to IEC / EN 60068-2-6)		Non-operating vibration (sinusoidal, 10 Hz to 2000 Hz, +/- 0.15 mm, 2 g)

2.7. Compliance

The COMe-bTL6 complies with the following or the latest status thereof. If modified, the prerequisites for specific approvals may no longer apply. For more information, contact Kontron Support.

Table 27: Compliance CE Mark

Europe – CE Mark	
Directives	**2014/30/EU:** Electromagnetic Compatibility **2014/35/EU**: Low Voltage **2011/65/EU**: RoHS II **2001/95/EC**: General Product Safety
EMC	**EN 55032 Class B** Electromagnetic compatibility of multimedia equipment- Emission Requirements Class A **EN61000-6-2** Electromagnetic compatibility (EMC) Part 6-2: Generic standards - Immunity standard for industrial environments
Safety	**EN 62368-1** Audio/video, information and communication technology equipment - Part 1: Safety requirements

Table 28: Country Compliance

USA/CANADA	
Safety	UL 62368-1 & CSA C22.2 No. 62368-1 (Component Recognition) Audio/video, information and communication technology equipment - Part 1: Safety requirements Recognized by Underwriters Laboratories Inc. Representative samples of this component have been evaluated by UL and meet applicable UL requirements. UL listings: AZOT2.E147705 AZOT8.E147705
UK CA Mark	
EMC	**BS EN 55032 Class B** Electromagnetic compatibility of multimedia equipment- Emission Requirements Class A **BS EN 61000-6-2** Electromagnetic compatibility (EMC) Part 6-2: Generic standards - Immunity standard for industrial environments
Safety	**BS EN 62368-1** Audio/video, information and communication technology equipment - Part 1: Safety requirements
CB scheme (For International Certifications)	
Safety	**IEC 62368-1** Audio/video, information and communication technology equipment - Part 1: Safety requirements

If the product is modified, the prerequisites for specific approvals may no longer apply.

Kontron is not responsible for any radio television interference caused by unauthorized modifications of the delivered product or the substitution or attachment of connecting cables and equipment other than those specified by Kontron. The correction of interference caused by unauthorized modification, substitution or attachment is the user's responsibility.

2.7.1. MTBF

The MTBF (Mean Time Before Failure) values were calculated using a combination of the manufacturer's test data, (if 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. This particular method takes into account varying temperature and stress data and the system is assumed to have not been burned-in. Other environmental stresses (such as extreme altitude, vibration, salt-water exposure) lower MTBF values.

Table 29: MTBF

MTBF
System MTBF (hour) = 554219 h @ 40°C for 38038-0000-26-2 (COMe-bTL6 Celeron 6600HE HM570E) Reliability report article number: 38038-0000-26-2
System MTBF (hour) = 490083 h @ 40°C for 38039-0010-47-0 (COMe-bTL6 E2 W-11865MRE RM590E) Reliability report article number: 38039-0010-47-0

The MTBF estimated value above assumes no fan, but a passive heat sinking arrangement. Estimated RTC battery life (as opposed to battery failures) is not accounted for and needs to be considered separately. Battery life depends on both temperature and operating conditions. When the module is connected to external power, the only battery drain is from leakage paths.

Figure 6 and Figure 7 show MTBF de-rating values for module variants when used in an office or telecommunications environment. Other environmental stresses (extreme altitude, vibration, salt-water exposure, etc.) lower MTBF values.

Figure 6: MTBF De-rating Values (Reliability report: 38038-0000-26-2)

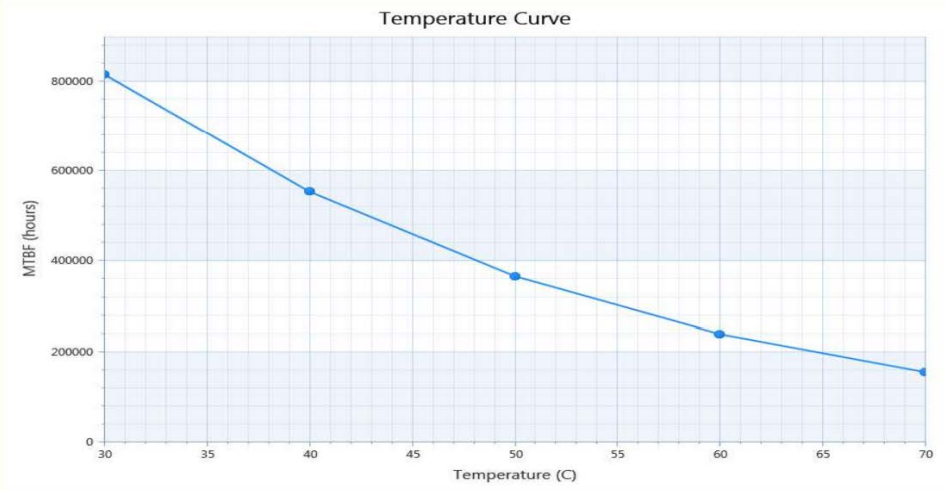
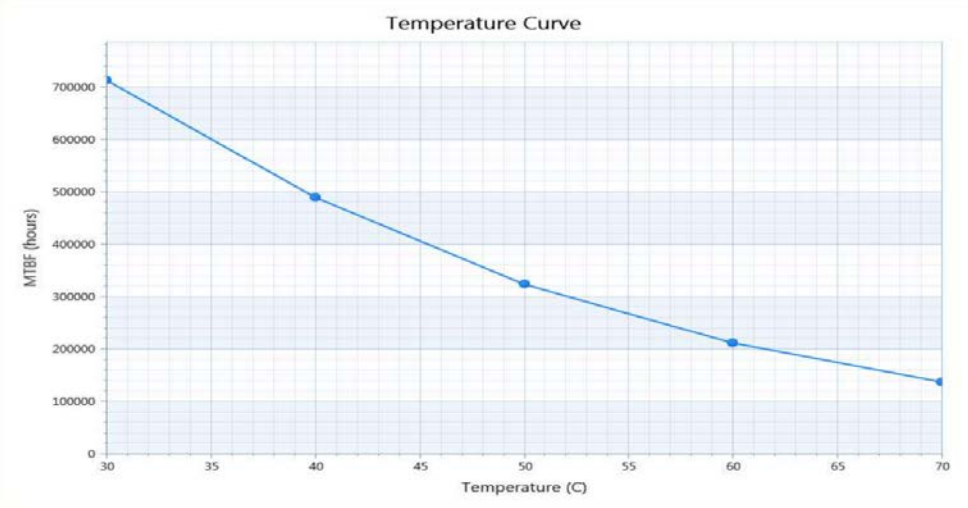


Figure 7: MTBF De-rating Values (Reliability report: 38039-0010-47-0)



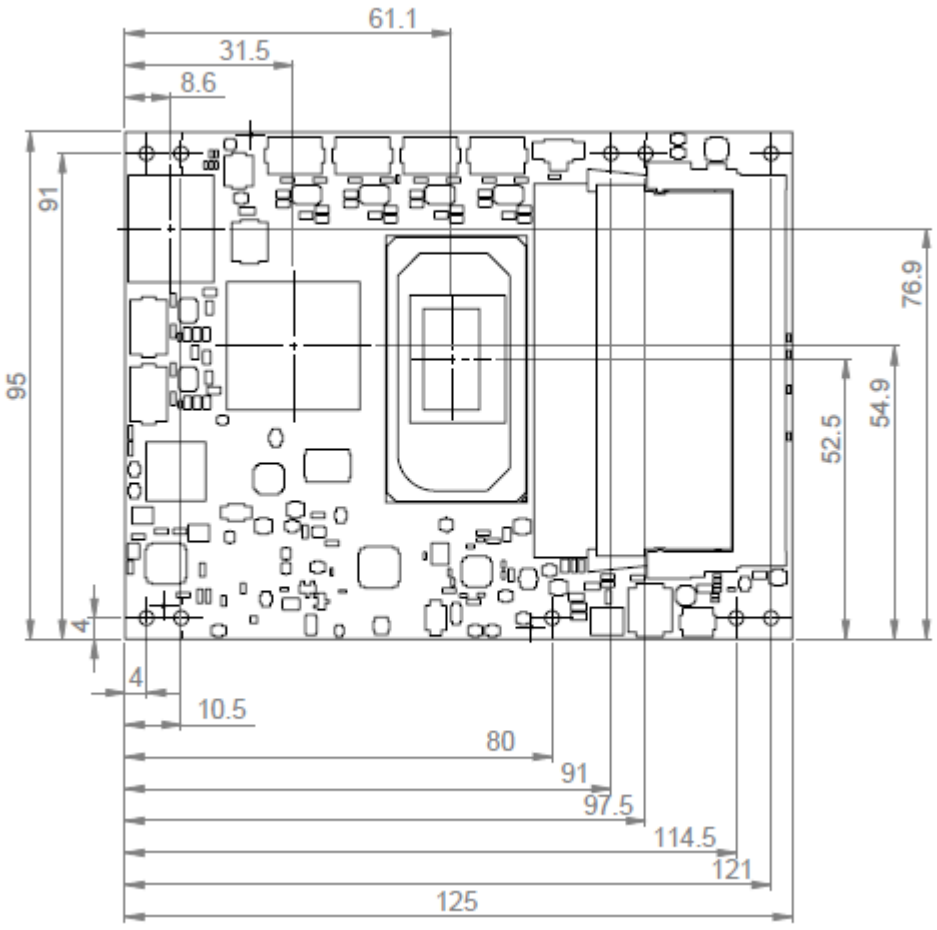
2.8. Mechanical Specification

The COMe-bTL6 is compliant with the COM Express® PICMG COM.0 Rev 3.0, mechanical specification.

2.8.1. Module Dimensions

The COMe basic module dimensions are 95 mm x 125 mm (3.7“x 4.9“).

Figure 8: Module Dimensions

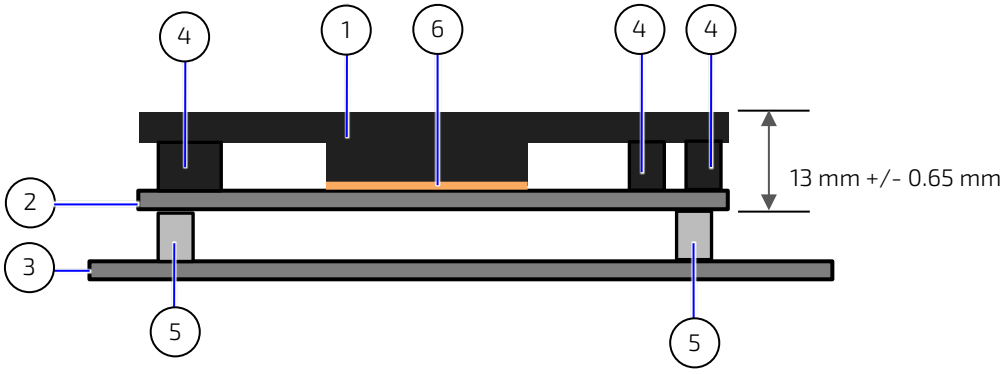


2.8.2. Module Height

The COM Express® specification defines a module height of approximately 13 mm, when measured from the bottom of the module's PCB board to the top of the heatspreader, see Figure 9: Module and Carrier Height.

The overall height of the module and carrier board depends on the implemented cooling solution. The height of the cooling solution is not specified in the COMe specification.

Figure 9: Module and Carrier Height

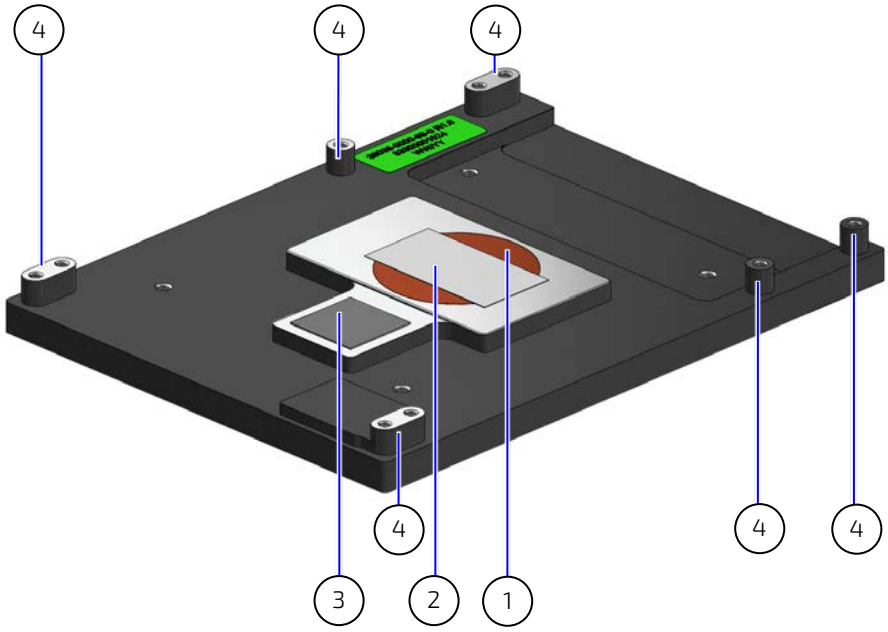


1 Heatspreader
2 Module PCB board
3 Carrier PCB board
4 Heatspreader standoff(s)
5 Connector standoff(s) 5 mm or 8 mm
6 Copper core and Thermal Interface Material (TIM)

2.8.3. Heatspreader Plate Assembly Dimensions

The module's cooling concept uses a heatspreader plate assembly 95 mm x 125 mm (3.7"x 4.9") fasten on the module via the heatspreader plate standoffs, see Figure 10, pos. 4. The heatspreader plate works as a COM Express® standard thermal interface and must be used with a heat sink or external cooling devices to maintain the heatspreader plate at proper operating temperatures. For module and heatspreader plate height information, see Chapter 2.8.2: Module Height.

Figure 10: Heatspreader Plate Assembly (viewed from bottom side)



1 Copper core
2 TIM Screen printed onto contact surface 0.1 to 0.15 mm thickness
3 TIM screen printed onto contact surface 0.25 mm +/- 0.05 mm
4 Heatspreader standoffs

3/ Features and Interfaces

3.1. ACPI Power States

ACPI enables the system to power down and save power when not required (suspend) and wake up when required (resume). The ACPI controls the power states S0-S5, where S0 has the highest priority and S5 the lowest priority.

The COMe-bTL6 supports ACPI 6.0 and the power states S0, S3, S4, S5 only.

Not all ACPI defined power states are available.
Systems that support the low-power idle state do not use power states S3 and S4.

Table 30: Supported Power States Function

S0	Working state
S3	ACPI suspend to RAM state
S4	Suspend-to-disk/Hibernate
S5	Soft-off state

To power on from states S3, S4 and S5 use:

- Power Button
- WakeOnLAN (S3, S4)

The OS must support wake up from a USB device and the carrier board must power the USB port with the standby voltage.

3.2. eSPI (option)

The eSPI interface from the PCH supports an external SIO and is pin shared with the LPC interface signal. To switch from one interface to another, requires a hardware modification in the form of additional resistors. The modules signal ESPI_EN# on pin-B47 indicates whether ESPI-mode or LPC-mode is enabled/disabled. The LPC interface is the default connection from the embedded controller to the COMe connector.

In eSPI mode "ESPI_EN#" connects to ground on the carrier. The module uses pull-up resistors on this signal to detect the mode.

If **ESPI_EN# selection on the carrier does not match the module configuration (eSPI/LPC) the module is unable to boot.**

3.3. Fast I2C

The internal I2C bus transfers data between components on the same module and the external I2C bus transfers data between I2C devices connected on the bus. The Fast I2C bus transfers data with rates up to 400 kHz.

To change the I2C bus speed, in the BIOS setup menu select:

Advanced>Miscellaneous>I2C Speed> 400 kHz to 1 kHz

The default speed is 200 kHz.

3.4. GPIO

The eight GPIO pins support four inputs pins (A54 for GPI0, A63 for GPI1, A67 for GPI2 and A85 for GPI3) and four output pins (A93 for GPO0, B54 for GPO1, B57 for GPO2 and B63 for GPO3) by default. The four GPI[0-3] pins are pulled high with a pull-up resistor (e.g. 100 K ohms) and the four GPO[0-3] pins are pulled low with a pull-down resistor (e.g. 100 K ohms) on the module.

To change the default GPIO signal-state users are required to make BIOS and/or OS-driver changes, and additional hardware changes by adding external termination resistors on the carrier board to override the weak on-module pull-up resistors with a lower resistance pull-down (e.g. 10 K ohms), or pull-down resistors with a lower resistance pull-up (e.g. 10 K ohms).

3.5. Hardware Monitor (HWM)

The Nuvoton NCT7802Y Hardware Monitor (HWM) controls the health of the system by monitoring critical aspects such as the module's processor temperature, power supply voltages (VCC /5 VSB), battery voltage V BAT and monitors and configures the on-board and external fans.

The HWM is accessible using the SM Bus address 5Ch, see Chapter 4.2: System Management (SM) Bus.

3.6. Intel® Optane™ (option)

The Intel® Optane™ memory technology accelerates system memory and storage system performance to improve the overall performance and responsiveness of high capacity workloads. Intel® Optane™ ensures that data which is used frequently resides on the fastest tier of storage.

Intel® Optane™ memory technology support is achieve using PCIe and is only possible with a custom BIOS. For more information, contact Kontron Support.

3.7. LPC

The Low Pin Count (LPC) interface is pin shared with eSPI, where the LPC interface is the default connection from the embedded controller to the COMe connector. To switch from one interface to another, requires a hardware modification in the form of additional resistors. The module's signal ESPI_EN# (pin-B47) indicates whether ESPI-mode or LPC-mode is enabled or disabled.

In LPC mode "ESPI_EN#" is unconnected on the carrier. The module uses pull-up resistors on this signal to detect the mode.

3.8. NVMe Storage (Option)

The NVMe SSD Flash memory supports up to one TByte. The optional NVMe SSD uses the four processor based 4.0 lanes that the chipset offers additionally to the 16 PCIe 4.0 lanes accessible via COMe PEG lines.

3.9. SMB

The System Management Bus (SMB) is a simple 2-wire bus for low-speed system management communication. The PCH controls the SMB. The module's SMB connects to the DDR4 memory and the hardware controller. For SMB address information, see Chapter 4.2 System Management (SM) Bus.

3.10. Real Time Clock (RTC)

The RTC keeps track of the current time accurately. The RTC's low power consumption enables the RTC to continue operation and keep time using a lower secondary source of power while the primary source of power is switched off or unavailable.

The COMe-bTL6 supports typical RTC values of 3 V and less than 10 µA. When powered by the mains power supply on-module regulators generate the RTC voltage, to reduce RTC current draw. The RTC's battery voltage range is 2.8 V to 3.47 V.

It is not recommended to run a system without a RTC battery on the carrier board. Even if the RTC battery is not required to keep the actual time and date when main power is off, a missing RTC battery will cause other side effects such as longer boot times. Intel processor environments are generally designed to rely on RTC battery voltage

3.11. Serial Peripheral Interface (SPI)

The Serial Peripheral Interface (SPI) bus is a synchronous serial data link where devices communicate in master/slave mode and the master device initiates the data frame. Multiple slave devices are allowed with individual slave select (chip select) lines.

The SPI interface may only be used with a SPI Flash device to boot from the external BIOS on the carrier board.

There is an option for a General Purpose SPI (GSPI) connection to COMe instead of the SPI interface for external Boot. GSPI. This requires a hardware modification in the form of additional resistors.

Table 31: GSPI/SPI Hardware Options

GSPI/SPI Hardware Options	COMe SPI Bus
Base module variant	Standard boot SPI bus
GSPI_HARDWIRED[1]	GSPI bus
GSPI_MUXED[1]	SPI/GSPI selectable by BIOS setting **Advanced> Miscellaneous> SPI lines active**

[1] Implemented on request only.

General purpose SPI connects to COMe instead of boot SPI and requires a hardware modification in the form of additional resistors. Implemented on request only

The COMe-bTL6 supports on-module and carrier board boot from SPI Flash. The SPI flash chip source is configured using the pins A34 (BIOS_DIS0#) and B88 (BIOS_DIS1#).

3.11.1. Booting the SPI Flash Chip

Initially, the EFI Shell is booted with an USB key containing the binary used to flash the on-module SPI Flash chip. To program the external SPI Flash chip on the carrier board with the BIOS binary, use an external programmer.

Register for Kontron's Customer Section to get access to BIOS downloads and PCN service.

To boot either the carrier board or on-module SPI flash chip, perform the following:

1. Connect a SPI flash with the correct size (similar to BIOS binary (*.BIN) file size) to the carrier SPI interface.

The external SPI flash chip on the carrier is required to be 32 MByte (256MBit).

2. Open pin A34 (BIOS_DIS0#) and connect pin B88 (BIOS_DIS1#) to ground to enable the external SPI Flash chip to boot on carrier SPI or ground pin A34 (BIOS_DIS0#), and open pin B88 (BIOS_DIS1#) to enable SPI Flash chip to boot on-module SPI.

The command line is EtaOemAfuX64.efi BTL6R110.bin /B /P /B /ME
In case of change, check Kontron's Customer Section for the latest BIOS binary package with reference command line.
ME must be disable in the BIOS setup before entering the command line: Advanced>PCH-FW Configuration> ME

3.11.2. SPI Boot

The SPI Flash device stores the boot BIOS. The COMe-bTL6 supports on-module and carrier board SPI Flash devices.

Optionally, an on-modules fail-safe second SPI flash can be implemented for additional safety, see Figure 1: Block Diagram COMe-bTL6. For more detailed information, contact Kontron Support.

The pins A34 (BIOS_DIS0#) and B88 (BIOS_DIS1#) configure the SPI Flash device as follows:

Table 32: SPI Boot Pin Configuration

BIOS_DIS0#	BIOS_DIS1#	Boot Bus	Function
Open	Open	SPI	Boot on on-module SPI
Open	GND	SPI	Boot on carrier board SPI

The BIOS cannot be split between two chips. Booting takes place either from the on-module SPI Flash chip or carrier board SPI Flash chip.

Table 33: Supported SPI Boot Flash

Size	Manufacturer	Part Number	Package Type
32 MByte (256 Mbit)	Winbond	W25Q256JVEIQ	WSON-8

3.11.3. External SPI Flash Boot on Modules with Intel® Management Engine

When booting from the external SPI Flash on the carrier board if the COM Express® module is exchanged for another module of the same type, the Intel® Management Engine (ME) will fail during the next start. The Management Engine (ME) binds itself to every module it has previously flashed which in the case of an external SPI Flash is the module present when flashed.

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

3.12. TCC (Time Coordinated Computing)

The Intel® Time Coordinated Computing (TCC) set of features supports real-time applications that need to deliver fast cycle times with low latency. The COMe-bTL6 supports selected Intel® TCC compatible processors, optimized for real-time applications. For information on the supported processor, see Table 6: 11th Generation Intel® Core™ Celeron® and Xeon® W Processor Spec.

To activate Intel® TCC Mode in the BIOS setup menu select: **Advanced> Intel® Time Coordination Computing> Intel® TCC Mode**). For more information, contact Kontron Support.

3.13. TPM 2.0

The Trusted Platform Module (TPM) 2.0 technology stores RSA encryption keys specific to the host system for hardware authentication

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

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

The COMe-bTL6 supports a TPM chip that connects directly to the PCH via a dedicated SPI interface.

3.14. TSN (option)

Time Sensitive Networking (TSN) is a set of international standards (IEEE-802.1 TSN), providing time synchronization and deterministic network communication features over standard Ethernet, thus leveraging the advantages of traditional Ethernet while meeting the timing and control needs of control and measurement applications.

As part of the Ethernet standard, TSN also benefits from continuing improvements in Ethernet security, bandwidth, and other capabilities and provides numerous advantages over today's standard Ethernet protocols. Time Sensitive Networking support can be used to connect to time sensitive (deterministic) networks according to IEEE-802.1 TSN.

The COMe-bTL6 uses one PCIe lane as a SGMII port to implement one 2.5 Base-T TSN capable Ethernet port.

TSN support is only available using the Intel® Mobile PCH-H "RM590E".

3.15. UART

The UART serial communications interface supports up to two serial RX/TX ports supplied by the chipset. The two serial ports are defined in the COMe specification on pins A98 (SERO_TX) and A99 (SERO_RX) for UART0, and pins A101 (SER1_TX) and A102 (SER1_RX) for UART1. Optionally it is possible that the two serial RX/TX ports are generated by the Embedded Controller.

Two serial RX/TX ports from the chipset (PCIe based, non-legacy, no RTS/CTS) with an option for two UART serial RX/TX ports from the Embedded Controller.

3.16. Watchdog Timer (WTD) Dual Stage

The watchdog timer interrupt is a hardware or software timer implemented by the module to the carrier board if there is a fault condition in the main program; the watchdog triggers a system reset or other corrective actions after a specific time, with the aim to bring the system back from a non-responsive to normal state.

The COMe-bTL6 supports an independently programmable watchdog that works with two stages that can be used stage by stage.

Table 34: Dual Staged Watchdog Timer- Time-Out Events

0000b	No action	Stage is off and will be skipped
0001b	Reset	Restarts the module and starts a new POST and operating system
0101b	Delay -> No action	Might be necessary when an operating system must be started and the time for the first trigger pulse must be extended. Only available in the first stage!
1000b	WDT Only	Triggers WDT pin on the carrier board connector (COM Express® pin B27) only
1001b	Reset + WDT	
1101b	DELAY + WDT -> No action	

3.16.1. Watchdog Timer Signal

The watchdog interrupt (WDT) on COM Express® pin B27 on COM Express® connector indicates a Watchdog time-out event has not been triggered within a set time. The WDT signal is configurable to any of the two stages. After reset, the signal is automatically de-asserted. If de-assertion is necessary during runtime, contact Kontron Support for further help.

3.17. XDP (option)

The XDP debug connector is used for development.

4/ System Resources

4.1. I2C Bus

The following table specifies the devices connected the accessible I2C bus including the I2C address. The I2C bus is available at the COM Express® connector pin B33, I2C_CK and pin B34, I2C_DAT.

Table 35: I2C Bus Port Address

8-bit Address	7-bit Address	Used For	Available
58h	2Ch	Internally reserved	No
A0h	50h	Module embedded EEPROM (Eeep)	Yes
AEh	57h	Carrier board EEPROM	Optional
64h	32h	External RTC	Optional

4.2. System Management (SM) Bus

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

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

The following table specifies the 8-bit and 7-bit SMBus write address for all devices.

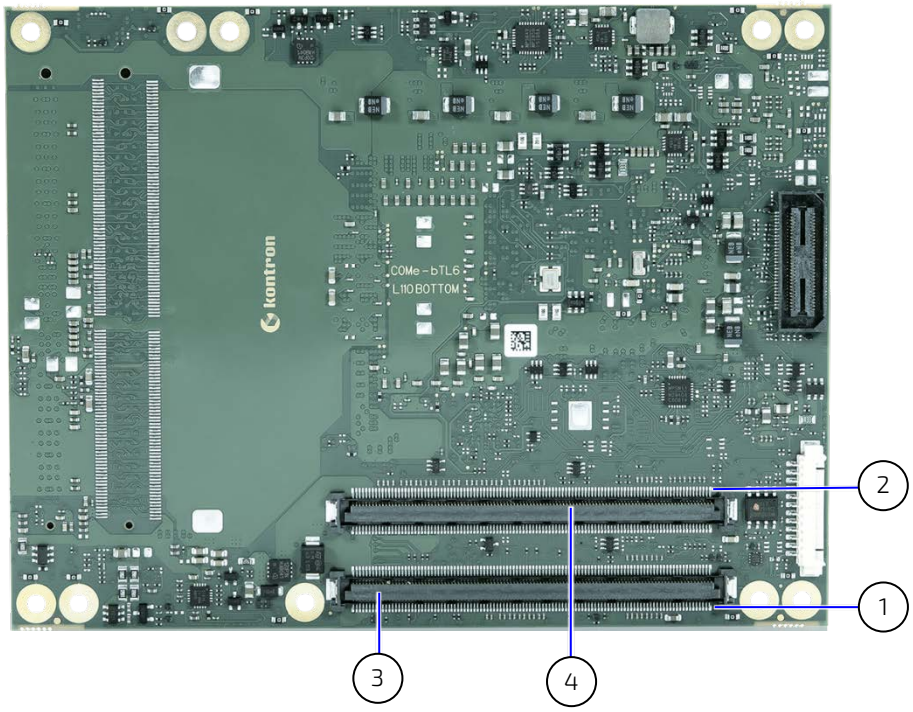
Table 36: SMBus Address

8-bit Address	7-bit Address	Device	Description
A0h	50h	DDR4 channel A EEPROM	SODIMM
A4h	52h	DDR4 channel B EEPROM	SODIMM
A6hh	53h	DDR4 Channel C EEPROM (only optional)	SODIMM (option)
5Ch	2Eh	Hardware Monitor NCT7802Y	Do not use this address for external devices under any circumstances

5/ COMe Interface Connector

The COMe-bTL6 is a COM Express® compact module containing two 220-pin connectors X1A and X1B; each with two rows called row A & B on the primary connector X1A and row C & D on the secondary connector X1B.

Figure 11: COMe Interface Connectors



1	COMe interface connector (X1A)	3	Pin X1A, PinA1
2	COMe Interface connector (X1B)	4	Pin X1B, Pin D1

5.1. Connecting COMe Interface Connector to Carrier Board

The COMe interface connectors (X1A, X1B) are inserted into the corresponding connectors on the carrier board and secured using the mounting points and standoffs. The height of the standoffs (either 5 mm or 8 mm) depends on the height of the carrier board's connector.

⚠CAUTION

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

Observe that only trained personnel aware of the associated dangers connect the module, within an access controlled ESD-safe workplace.

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/EN 62368

5.2. X1A and X1B Signals

For a description of the terms used in the X1A and X1B pin assignment tables, see Table 37: General Signal Description. If a more detailed pin assignment description is required, refer to the PICMG COM.0 Rev. 3.0 Type 6 standard.

The information provided under type, module terminations and comments is complimentary to the COM.0 Rev 2.1 Type 6 standard. For more information, contact Kontron Support.

Table 37: General Signal Description

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

NOTICE

The pin assignment tables list the internal pull-ups (PU) or pull-downs (PD) implemented by the chip vendors.

5.3. Connector (X1A) Row A1 – A110

The following tables list the pin assignment of the 220-pin connector X1A (A1 to A110) and (Row B1 to B110) and connector X1B (C1 to C110) and (Row D1 to D110).

Table 38: Connector (X1A) Row A1 to A110 Pin Assignment

Pin	Signal	Description	Type	Termination	Comment
A1	GND	Power Ground	PWR GND	---	---
A2	GBE0_MDI3_-	Ethernet Media Dependent Interface 3 -	DP-I/O	---	---
A3	GBE0_MDI3_+	Ethernet Media Dependent Interface 3 +	DP-I/O	---	---
A4	GBE0_LINK_MID#	Ethernet Speed LED indicating 100Mbit and 1Gbit connection	OD	---	---
A5	GBE0_LINK_MAX#	Ethernet Speed LED indicating 2.5Gbit connection	OD	---	---
A6	GBE0_MDI2_-	Ethernet Media Dependent Interface 2 -	DP-I/O	---	---
A7	GBE0_MDI2_+	Ethernet Media Dependent Interface 2 +	DP-I/O	---	---
A8	GBE0_LINK#	LAN Link LED	OD	---	---

Pin	Signal	Description	Type	Termination	Comment
A9	GBE0_MDI1_-	Ethernet Media Dependent Interface 1 -	DP-I/O	---	---
A10	GBE0_MDI1_+	Ethernet Media Dependent Interface 1 +	DP-I/O	---	---
A11	GND	Power Ground	PWR GND	---	---
A12	GBE0_MDI0_-	Ethernet Media Dependent Interface 0 -	DP-I/O	---	---
A13	GBE0_MDI0_+	Ethernet Media Dependent Interface 0 +	DP-I/O	---	---
A14	V_GBE0_CTREF	Center Tab Reference Voltage	O	---	100nF capacitor to GND
A15	PM_SLP_S3#	Suspend To RAM (or deeper) Indicator	O-3.3	PD 10k	---
A16	SATA0_TX_+	SATA Transmit Pair 0 +	DP-O	---	---
A17	SATA0_TX_-	SATA Transmit Pair 0 -	DP-O	---	---
A18	PM_SLP_S4#	Suspend To Disk (or deeper) Indicator	O-3.3	PD 10k	---
A19	SATA0_RX_+	SATA Receive Pair 0 +	DP-I	---	---
A20	SATA0_RX_-	SATA Receive Pair 0 -	DP-I	---	---
A21	GND	Power Ground	PWR GND	---	---
A22	SATA2_TX_+	SATA Transmit Pair 2 +	DP-O	---	---
A23	SATA2_TX_-	SATA Transmit Pair 2 -	DP-O	---	---
A24	PM_SLP_S5#	Soft Off Indicator	O-3.3	PD 10k	---
A25	SATA2_RX_+	SATA Receive Pair 2 +	DP-I	---	---
A26	SATA2_RX_-	SATA Receive Pair 2 -	DP-I	---	---
A27	BATLOW#	Battery Low	I-3.3	PU 10k 3.3V (S5)	Assertion will prevent wake from S3-S5 state
A28	SATA_ACT#	Serial ATA activity LED	OD-3.3	PU 10k 3.3V (S0)	Can sink 15mA
A29	HDA_SYNC	HD Audio Sync	O-3.3	---	---
A30	HDA_RST#	HD Audio Reset	O-3.3	---	---
A31	GND	Power Ground	PWR GND	---	---
A32	HDA_BITCLK	HD Audio Bit Clock Output	O-3.3	---	---
A33	HDA_SDOUT	HD Audio Serial Data Out	O-3.3	---	---
A34	BIOS_DIS0#/ESPI_SAFS	BIOS Selection Strap 0	I-3.3	PU 10k 3.3V (S5)	---
A35	THRMTRIP#	Thermal Trip	O-3.3	PU 10k 3.3V (S0)	Thermal Trip Event, transition to S5 indicator
A36	USB6_-	USB 2.0 Data Pair Port 6 –	DP-I/O	PD 14.25k to 24.8k in PCH	---
A37	USB6_+	USB 2.0 Data Pair Port 6 +	DP-I/O	PD 14.25k to 24.8k in PCH	---
A38	USB_6_7_OC#	USB Overcurrent Indicator Port 6/7	I-3.3	PU 10k 3.3V (S5)	---
A39	USB4_-	USB 2.0 Data Pair Port 4 -	DP-I/O	PD 14.25k to 24.8k in PCH	---

Pin	Signal	Description	Type	Termination	Comment
A40	USB4_+	USB 2.0 Data Pair Port 4 +	DP-I/O	PD 14.25k to 24.8k in PCH	---
A41	GND	Power Ground	PWR GND	---	---
A42	USB2_-	USB 2.0 Data Pair Port 2 –	DP-I/O	PD 14.25k to 24.8k in PCH	---
A43	USB2_+	USB 2.0 Data Pair Port 2 +	DP-I/O	PD 14.25k to 24.8k in PCH	---
A44	USB_2_3_OC#	USB Overcurrent Indicator Port 2/3	I-3.3	PU 10k 3.3V (S5)	---
A45	USB0_–	USB 2.0 Data Pair Port 0 –	DP-I/O	PD 14.25k to 24.8k in PCH	---
A46	USB0_+	USB 2.0 Data Pair Port 0 +	DP-I/O	PD 14.25k to 24.8k in PCH	---
A47	V_3V0_RTC	Real-Time Clock Circuit Power Input	PWR 3V	---	Voltage range 2.8 V - 3.47 V
A48	NC	Reserved for future use	NC	---	RSVD
A49	GBE0_SDP	Gigabit Ethernet Controller 0 Software-Definable Pin	I/O-3.3	---	---
A50	LPC_SERIRQ_ESPI_CS1#	Serial Interrupt Request / eSPI Master Chip Select 1	I/OD-3.3 / O-1.8	PU 8k2 3.3V (S0)	LPC only
A51	GND	Power Ground	PWR GND	---	---
A52	PCIE_TX5_+	PCI Express Lane 5 Transmit +	DP-O	---	---
A53	PCIE_TX5_-	PCI Express Lane 5 Transmit -	DP-O	---	---
A54	GPI0	General Purpose Input 0	I-3.3	PU 100k 3.3V (S0)	---
A55	PCIE_TX4_+	PCI Express Lane 4 Transmit +	DP-O	---	---
A56	PCIE_TX4_-	PCI Express Lane 4 Transmit -	DP-O	---	---
A57	GND	Power Ground	PWR GND	---	---
A58	PCIE_TX3_+	PCI Express Lane 3 Transmit +	DP-O	---	---
A59	PCIE_TX3_-	PCI Express Lane 3 Transmit -	DP-O	---	---
A60	GND	Power Ground	PWR GND	---	---
A61	PCIE_TX2_+	PCI Express Lane 2 Transmit +	DP-O	---	---
A62	PCIE_TX2_-	PCI Express Lane 2 Transmit -	DP-O	---	---
A63	GPI1	General Purpose Input 1	I-3.3	PU 100k 3.3V (S0)	---
A64	PCIE_TX1_+	PCI Express Lane 1 Transmit +	DP-O	---	---
A65	PCIE_TX1_-	PCI Express Lane 1 Transmit -	DP-O	---	---
A66	GND	Power Ground	PWR GND	---	---
A67	GPI2	General Purpose Input 2	I-3.3	PU 100k 3.3V (S0)	---
A68	PCIE_TX0_+	PCI Express Lane 0 Transmit +	DP-O	---	---
A69	PCIE_TX0_-	PCI Express Lane 0 Transmit -	DP-O	---	---
A70	GND	Power Ground	PWR GND	---	---
A71	LVDS_A_DATA0_EDP_TX2_+	LVDS Channel A DAT0+ / EDP Lane 2 Transmit +	DP-O	---	---

Pin	Signal	Description	Type	Termination	Comment
A72	LVDS_A_DATA0_EDP_TX2_-	LVDS Channel A DAT0- / EDP Lane 2 Transmit -	DP-O	---	---
A73	LVDS_A_DATA0_EDP_TX1_+	LVDS Channel A DAT1+ / EDP Lane 1 Transmit +	DP-O	---	---
A74	LVDS_A_DATA0_EDP_TX1_-	LVDS Channel A DAT1- / EDP Lane 1 Transmit -	DP-O	---	---
A75	LVDS_A_DATA0_EDP_TX0_+	LVDS Channel A DAT2+ / EDP Lane 0 Transmit +	DP-O	---	---
A76	LVDS_A_DATA0_EDP_TX0_-	LVDS Channel A DAT2- / EDP Lane 0 Transmit -	DP-O	---	---
A77	LVDS_VDD_EN	LVDS / EDP Panel Power Control	O-3.3	PD 100k	---
A78	LVDS_A_DATA3_+	LVDS Channel A DAT3+	DP-O	---	---
A79	LVDS_A_DATA3_-	LVDS Channel A DAT3-	DP-O	---	---
A80	GND	Power Ground	PWR GND	---	---
A81	LVDS_A_CLK_EDP_TX3_+	LVDS Channel A Clock+ / EDP Lane 3 Transmit +	DP-O	---	Clock: 20 -80MHz
A82	LVDS_A_CLK_EDP_TX3_-	LVDS Channel A Clock- / EDP Lane 3 Transmit -	DP-O	---	Clock: 20-80MHz
A83	LVDS_DDC_CLK_EDP_AUX_+	LVDS I2C Clock (DDC) / EDP AUX +	I/O-3.3	PU 2k2 3.3V (S0)	---
A84	LVDS_DDC_CLK_EDP_AUX_-	LVDS I2C Data (DDC) / EDP AUX -	I/O-3.3	PU 2k2 3.3V (S0)	---
A85	GPI3	General Purpose Input 3	I-3.3	PU 100k 3.3V (S0)	---
A86	SPI_CS2_TPM_EXT#	Reserved for future use	NC	---	Untested feature
A87	EDP_HPD	EDP Hot Plug Detect	I-3.3	PD 400k LVDS / 100k EDP	---
A88	CLK_100M_PCIE_+	Reference PCI Express Clock +	DP-O	---	100MHz
A89	CLK_100M_PCIE_-	Reference PCI Express Clock -	DP-O	---	100MHz
A90	GND	Power Ground	PWR GND	---	---
A91	V_3V3_SPI	3.3V Power Output Pin for external SPI flash	O-3.3	---	100mA (max.)
A92	SPI_MISO	SPI Master IN Slave OUT	I-3.3	PU 15k-40k in PCH (S5)	All SPI signals are tri-stated until reset is deasserted.
A93	GPO0	General Purpose Output 0	O-3.3	PD 100k	---
A94	SPI_CLK	SPI Clock	O-3.3	PU 15k-40k in PCH (S5)	All SPI signals are tri-stated with 20k ohm CPU internal weak pull-up until reset is deasserted.
A95	SPI_MOSI	SPI Master Out Slave In	O-3.3	PU 15k-40k in PCH (S5)	All SPI signals are tri-stated with 20k ohm CPU internal weak pull-up until reset is deasserted.
A96	TPM_PP	TPM Physical Presence	I-3.3	PD 10k	TPM does not use this functionality
A97	NC	Indicates TYPE10# to carrier board	NC	---	NC for type 6

Pin	Signal	Description	Type	Termination	Comment
A98	SER0_TX	Serial Port 0 TXD	O-3.3	---	20V protection circuit implemented on module, PD on carrier board needed for proper operation.
A99	SER0_RX	Serial Port 0 RXD	I-5T	PU 47k 3.3V (S0)	20V protection circuit implemented on module.
A100	GND	Power Ground	PWR GND	---	---
A101	SER1_TX	Serial Port 1 TXD	O-3.3	---	20V protection circuit implemented on module, PD on carrier board needed for proper operation
A102	SER1_RX	Serial Port 1 RXD	I-5T	PU 47k 3.3V (S0)	20V protection circuit implemented on module
A103	EXT_LID#	LID Switch Input	I-3.3	PU 47k 3.3V (S5)	20V protection circuit implemented on module
A104	V_IN_VAR	Main Input Voltage (4.75V-20V)	PWR 4.75-20V	---	---
A105	V_IN_VAR	Main Input Voltage (4.75V-20V)	PWR 4.75-20V	---	---
A106	V_IN_VAR	Main Input Voltage (4.75V-20V)	PWR 4.75-20V	---	---
A107	V_IN_VAR	Main Input Voltage (4.75V-20V)	PWR 4.75-20V	---	---
A108	V_IN_VAR	Main Input Voltage (4.75V-20V)	PWR 4.75-20V	---	---
A109	V_IN_VAR	Main Input Voltage (4.75V-20V)	PWR 4.75-20V	---	---
A110	GND	Power Ground	PWR GND	---	---

5.4. Connector (X1A) Row B1 - B110

Table 39: Connector (X1A) Row B1 to B110 Pin Assignment

Pin	Signal	Description	Type	Termination	Comment
B1	GND	Power Ground	PWR GND	---	---
B2	GBE0_ACT#	Ethernet Activity LED	OD	---	---
B3	LPC_FRAME#_ESPI _CS0#	LPC Frame Indicator / eSPI Master Chip Select 0	O-3.3 / eSPI O-1.8	---	LPC only
B4	LPC_AD0_ESPI_IO_ 0	LPC Multiplexed Command, Address & Data 0 / eSPI Master Data I/O 0	I/O-3.3 / eSPI I/O-1.8	PU 15k-40k in PCH (S5)	LPC only
B5	LPC_AD1_ESPI_IO_1	LPC Multiplexed Command, Address & Data 1 / eSPI Master Data I/O 1	I/O-3. 3 / eSPI I/O-1.8	PU 15k-40k in PCH (S5)	LPC only
B6	LPC_AD2_ESPI_IO_ 2	LPC Multiplexed Command, Address & Data 2 / eSPI Master Data I/O 2	I/O-3. 3 / eSPI I/O-1.8	PU 15k-40k in PCH (S5)	LPC only
B7	LPC_AD3_ESPI_IO_ 3	LPC Multiplexed Command, Address & Data 3 / eSPI Master Data I/O 3	I/O-3. 3 / eSPI I/O-1.8	PU 15k-40k in PCH (S5)	LPC only
B8	LPC_DRQ0#_ESPI_ ALERT0#	LPC Serial DMA/Master Request 0 / eSPI Alert 0	I-3.3 / eSPI I-1.8	---	LPC only
B9	LPC_DRQ1#_ESPI_ ALERT1#	LPC Serial DMA/Master Request 1 / eSPI Alert 1	I-3.3 / eSPI I-1.8	---	LPC only
B10	LPC_CLK_ESPI_CLK	24MHz LPC clock	O-3.3 / eSPI O-1.8	PD 20k in PCH	24.MHz
B11	GND	Power Ground	PWR GND	---	---
B12	PWRBTN#	Power Button	I-3.3	PU 10k 3.3V (S5)	---
B13	SMB_CLK	SMBUS Clock	O-3.3	PU 3k74 3.3V (S5)	---
B14	SMB_DAT	SMBUS Data	I/O-3.3	PU 3k74 3.3V (S5)	---
B15	SMB_ALERT#	SMBUS Alert	I/O-3.3	PU 2k2 3.3V (S5)	---
B16	SATA1_TX_+	SATA 1 Transmit Pair +	DP-O	---	---
B17	SATA1_TX_-	SATA 1 Transmit Pair -	DP-O	---	---
B18	SUS_STAT#_ESPI_ RESET#	Suspend Status / eSPI Reset	O-3.3 / O-1.8	PD 10K	---
B19	SATA1_RX_+	SATA 1 Receive Pair +	DP-I	---	---
B20	SATA1_RX_-	SATA 1 Receive Pair -	DP-I	---	---
B21	GND	Power Ground	PWR GND	---	---
B22	SATA3_TX_+	SATA 3 Transmit Pair +	DP-O	---	---
B23	SATA3_TX_-	SATA 3 Transmit Pair -	DP-O	---	---
B24	PWR_OK	Power OK	I-5T	PU 61k 3.3V	20V protection circuit implemented on module
B25	SATA3_RX_+	SATA 3 Receive Pair +	DP-I	---	---

Pin	Signal	Description	Type	Termination	Comment
B26	SATA3_RX_-	SATA 3 Receive Pair -	DP-I	---	---
B27	WDT	Watch Dog Time-Out event	O-3.3	PD 10K	---
B28	NC (SNDW_CLK option)	Not Connected	NC	---	Untested option to support Soundwire bus.
B29	HDA_SDIN1_SNDW_DATA	Audio Codec Serial Data in 1	I-3.3	PD 20k in PCH	Untested option to support Soundwire bus.
B30	HDA_SDIN0	Audio Codec Serial Data in 0	I-3.3	PD 20k in PCH	---
B31	GND	Power Ground	PWR GND	---	---
B32	SPKR	Speaker	O-3.3	PD 20k in PCH	PD is enabled until reset is deasserted
B33	I2C_CLK	I2C Clock	O-3.3	PU 2k21 3.3V (S5)	---
B34	I2C_DAT	I2C Data	I/O-3.3	PU 2k21 3.3V (S5)	---
B35	THRM#	Over Temperature Input	I-3.3	PU 10k 3.3V (S0)	No function implemented.
B36	USB7_-	USB 2.0 Data Pair Port 7 –	DP-I/O	PD 14.25k to 24.8k in PCH	---
B37	USB7_+	USB 2.0 Data Pair Port 7 +	DP-I/O	PD 14.25k to 24.8k in PCH	---
B38	USB_4_5_OC#	USB Overcurrent Indicator Port 4/5	I-3.3	PU 10k 3.3V (S5)	---
B39	USB5_-	USB 2.0 Data Pair Port 5 –	DP-I/O	PD 14.25k to 24.8k in PCH	---
B40	USB5_+	USB 2.0 Data Pair Port 5 +	DP-I/O	PD 14.25k to 24.8k in PCH	---
B41	GND	Power Ground	PWR GND	---	---
B42	USB3_-	USB 2.0 Data Pair Port 3 –	DP-I/O	PD 14.25k to 24.8k in PCH	---
B43	USB3_+	USB 2.0 Data Pair Port 3 +	DP-I/O	PD 14.25k to 24.8k in PCH	---
B44	USB_0_1_OC#	USB Overcurrent Indicator Port 0/1	I-3.3	PU 10k 3.3V (S5)	---
B45	USB1_-	USB 2.0 Data Pair Port 1 –	DP-I/O	PD 14.25k to 24.8k in PCH	---
B46	USB1_+	USB 2.0 Data Pair Port 1 +	DP-I/O	PD 14.25k to 24.8k in PCH	---
B47	ESPI_EN#	Enable/Disable ESPI-Mode/LPC-Mode	I-3.3	PU 20k 3.3V (S5)	---
B48	USB_HOST_PRSNT	USB Host Detection	I-3.3	PD 100k	---
B49	EXT_SYS_RESET#	Reset Button Input	I-3.3	PU 10k 3.3V (S5)	---
B50	CB_RESET#	Carrier Board Reset	O-3.3	PD 10k	---
B51	GND	Power Ground	PWR GND	---	---
B52	PCIE_RX5_+	PCI Express Lane 5 Receive +	DP-I	---	---
B53	PCIE_RX5_-	PCI Express Lane 5 Receive -	DP-I	---	---
B54	GPO1	General Purpose Output 1	O-3.3	PD 100k	---
B55	PCIE_RX4_+	PCI Express Lane 4 Receive +	DP-I	---	---
B56	PCIE_RX4_-	PCI Express Lane 4 Receive -	DP-I	---	---
B57	GPO2	General Purpose Output 2	O-3.3	PD 100k	---

Pin	Signal	Description	Type	Termination	Comment
B58	PCIE_RX3_+	PCI Express Lane 3 Receive +	DP-I	---	---
B59	PCIE_RX3_-	PCI Express Lane 3 Receive -	DP-I	---	---
B60	GND	Power Ground	PWR GND	---	---
B61	PCIE_RX2_+	PCI Express Lane 2 Receive +	DP-I	---	---
B62	PCIE_RX2_-	PCI Express Lane 2 Receive -	DP-I	---	---
B63	GPO3	General Purpose Output 3	O-3.3	PD 100k	---
B64	PCIE_RX1_+	PCI Express Lane 1 Receive +	DP-I	---	---
B65	PCIE_RX1_-	PCI Express Lane 1 Receive -	DP-I	---	---
B66	WAKE0#	PCI Express Wake Event	I-3.3	PU 10k 3.3V (S5)	---
B67	WAKE1#	General Purpose Wake Event	I-3.3	PU 10k 3.3V (S5)	---
B68	PCIE_RX0_+	PCI Express Lane 0 Receive +	DP-I	---	---
B69	PCIE_RX0_-	PCI Express Lane 0 Receive -	DP-I	---	---
B70	GND	Power Ground	PWR GND	---	---
B71	LVDS_B_DATA0_EDP2_TX2_+	LVDS Channel B DAT0+	DP-O	---	Option for second eDP port
B72	LVDS_B_DATA0_EDP2_TX2_-	LVDS Channel B DAT0-	DP-O	---	Option for second eDP port
B73	LVDS_B_DATA1_EDP2_TX1_+	LVDS Channel B DAT1+	DP-O	---	Option for second eDP port
B74	LVDS_B_DATA1_EDP2_TX1_-	LVDS Channel B DAT1-	DP-O	---	Option for second eDP port
B75	LVDS_B_DATA2_EDP2_TX0_+	LVDS Channel B DAT2+	DP-O	---	Option for second eDP port
B76	LVDS_B_DATA2_EDP2_TX0_-	LVDS Channel B DAT2-	DP-O	---	Option for second eDP port
B77	LVDS_B_DATA3_EDP2_AUX_+	LVDS Channel B DAT3+	DP-O	---	Option for second eDP port
B78	LVDS_B_DATA3_EDP2_AUX_-	LVDS Channel B DAT3-	DP-O	---	Option for second eDP port
B79	LVDS_EDP_BKLT_EN	LVDS / EDP Panel Backlight On	O-3.3	PD 100k	---
B80	GND	Power Ground	PWR GND	---	---
B81	LVDS_B_CLK_EDP2_TX3_+	LVDS Channel B Clock+	DP-O	---	20-80MHz
B82	LVDS_B_CLK_EDP2_TX3_-	LVDS Channel B Clock-	DP-O	---	20-80MHz
B83	LVDS_BKLT_CTRL	LVDS / EDP Backlight Brightness Control	O-3.3	---	---
B84	V_IN_5V0_S5	5V Standby	PWR 5V (S5)	---	Optional: not necessary in single supply mode.
B85	V_IN_5V0_S5	5V Standby	PWR 5V (S5)	---	Optional: not necessary in single supply mode.
B86	V_IN_5V0_S5	5V Standby	PWR 5V (S5)	---	Optional: not necessary in single supply mode.
B87	V_IN_5V0_S5	5V Standby	PWR 5V (S5)	---	Optional: not necessary in single supply mode.

Pin	Signal	Description	Type	Termination	Comment
B88	BIOS_DIS1#	BIOS Selection Strap 1	I-3.3	PU 10k 3.3V (S0)	PU might be powered during suspend.
B89	VGA_RED	Analog Video RGB-RED	NC	---	Optional
B90	GND	Power Ground	PWR GND	---	---
B91	VGA_GRN	Analog Video RGB-GREEN	NC	---	Optional
B92	VGA_BLU	Analog Video RGB-BLUE	NC	---	Optional
B93	VGA_HSYNC	Analog Video H-Sync	NC	---	Optional
B94	VGA_VSYNC	Analog Video V-Sync	NC	---	Optional
B95	VGA_I2C_CK	Display Data Channel Clock	NC	---	Optional
B96	VGA_I2C_DATA	Display Data Channel Data	NC	---	Optional
B97	SPI_CS#	SPI Chip Select	O-3.3	---	---
B98	NC	Reserved for future use	NC	---	RSVD
B99	NC	Reserved for future use	NC	---	RSVD
B100	GND	Power Ground	PWR GND	---	---
B101	FAN_PWMOUT	Fan PWM Output	O-3.3	---	20V protection circuit implemented on module, PD on carrier board needed for proper operatio
B102	FAN_TACHIN	Fan Tach Input	I-3.3	PU 47k 3.3V (S0)	20V protection circuit implemented on modul
B103	EXT_SLEEP#	Sleep Button Input	I-3.3	PU 47k 3.3V (S5)	20V protection circuit implemented on modul
B104	V_IN_VAR	Main Input Voltage (4.75V-20V)	PWR 4.75-20V	---	---
B105	V_IN_VAR	Main Input Voltage (4.75V-20V)	PWR 4.75-20V	---	---
B106	V_IN_VAR	Main Input Voltage (4.75V-20V)	PWR 4.75-20V	---	---
B107	V_IN_VAR	Main Input Voltage (4.75V-20V)	PWR 4.75-20V	---	---
B108	V_IN_VAR	Main Input Voltage (4.75V-20V)	PWR 4.75-20V	---	---
B109	V_IN_VAR	Main Input Voltage (4.75V-20V)	PWR 4.75-20V	---	---
B110	GND	Power Ground	PWR GND	---	---

5.5. Connector (X1B) Row C1 - C110

Table 40: Connector (X1B) Row C1 to C110 Pin Assignment

Pin	Signal	Description	Type	Termination	Comment
C1	GND	Power Ground	PWR GND	---	---
C2	GND	Power Ground	PWR GND	---	---
C3	USB_SSRX0_-	USB Super Speed Receive 0 -	DP-I	---	---
C4	USB_SSRX0_+	USB Super Speed Receive 0 +	DP-I	---	---
C5	GND	Power Ground	PWR GND	---	---
C6	USB_SSRX1_-	USB Super Speed Receive 1 -	DP-I	---	---
C7	USB_SSRX1_+	USB Super Speed Receive 1 +	DP-I	---	---
C8	GND	Power Ground	PWR GND	---	---
C9	USB_SSRX2_-	USB Super Speed Receive 2 -	DP-I	---	---
C10	USB_SSRX2_+	USB Super Speed Receive 2 +	DP-I	---	---
C11	GND	Power Ground	PWR GND	---	---
C12	USB_SSRX3_-	USB Super Speed Receive 3 -	DP-I	---	---
C13	USB_SSRX3_+	USB Super Speed Receive 3 +	DP-I	---	---
C14	GND	Power Ground	PWR GND	---	---
C15	DDI1_TBT_LSX0_TXD	Not Connected	NC	---	---
C16	DDI1_TBT_LSX0_RXD	Not Connected	NC	---	---
C17	USB4_RT_ENA	Not Connected	NC	---	Untested option for possible USB4 implementation.
C18	NC	Reserved for future use	NC	---	RSVD
C19	PCIE_RX6_+	PCI Express Lane 6 Receive +	DP-I	---	---
C20	PCIE_RX6_-	PCI Express Lane 6 Receive -	DP-I	---	---
C21	GND	Power Ground	PWR GND	---	---
C22	PCIE_RX7_+	PCI Express Lane 7 Receive +	DP-I	---	---
C23	PCIE_RX7_-	PCI Express Lane 7 Receive -	DP-I	---	---
C24	DDI1_HPD	DDI1 Hotplug Detect	I-3.3	PD 100k	
C25	SML0_CLK	Not Connected	NC	---	Untested option for possible SMLink bus implementation.
C26	SML0_DAT	Not Connected	NC	---	Untested option for possible SMLink bus implementation.
C27	SML1_CLK	Not Connected	NC	---	Untested option for possible SMLink bus implementation.
C28	SML1_DAT	Not Connected	NC	---	Untested option for possible SMLink bus implementation.
C29	USB4_PD_I2C_CLK	Not Connected	NC	---	Untested option for possible USB4 implementation.

Pin	Signal	Description	Type	Termination	Comment
C30	USB4_PD_I2C_DAT	Not Connected	NC	---	Untested option for possible USB4 implementation.
C31	GND	Power Ground	PWR GND	---	---
C32	DDI2_DDCCLK_AUX_+	DDI2 CTRLCLK/AUX+	I/O-3.3	PD 100k	---
C33	DDI2_DDCDATA_AUX_-	DDI2 CTRLDATA/AUX-	I/O-3.3	PU 100k 3.3V (S0)	---
C34	DDI2_DDC_AUX_SEL	DDI2 DDC/AUX select	I-3.3	PD 1M	---
C35	DDI2_TBT_LSX1_TXD	Not connected	NC	---	Untested option for possible Thunderbolt implementation.
C36	DDI3_DDCCLK_AUX_+	DDI3 CTRLCLK/AUX+	I/O-3.3	PD 100k	---
C37	DDI3_DDCDATA_AUX_-	DDI3 CTRLDATA/AUX-	I/O-3.3	PU 100k 3.3V (S0)	---
C38	DDI3_DDC_AUX_SEL	DDI3 DDC/AUX select	I-3.3	PD 1M	---
C39	DDI3_PAIR0_+	DDI3 Pair 0 +	DP-O	---	---
C40	DDI3_PAIR0_-	DDI3 Pair 0 -	DP-O	---	---
C41	GND	Power Ground	PWR GND	---	---
C42	DDI3_PAIR1_+	DDI3 Pair 1 +	DP-O	---	---
C43	DDI3_PAIR1_-	DDI3 Pair 1 -	DP-O	---	---
C44	DDI3_HPD	DDI3 Hotplug Detect	I-3.3	PD 100k	---
C45	NC	Reserved for future use	NC	---	RSVD
C46	DDI3_PAIR2_+	DDI3 Pair 2 +	DP-O	---	---
C47	DDI3_PAIR2_-	DDI3 Pair 2 -	DP-O	---	---
C48	NC	Reserved for future use	NC	---	RSVD
C49	DDI3_PAIR3_+	DDI3 Pair 3 +	DP-O	---	---
C50	DDI3_PAIR3_-	DDI3 Pair 3 -	DP-O	---	---
C51	GND	Power Ground	PWR GND	---	---
C52	PEG_RX0_+	PEG Lane 0 Receive +	DP-I	---	---
C53	PEG_RX0_-	PEG Lane 0 Receive -	DP-I	---	---
C54	NC	NC for type 6 module	NC	---	TYPE0#
C55	PEG_RX1_+	PEG Lane 1 Receive +	DP-I	---	---
C56	PEG_RX1_-	PEG Lane 1 Receive -	DP-I	---	---
C57	NC	NC for type 6 module	NC	---	TYPE1#
C58	PEG_RX2_+	PEG Lane 2 Receive +	DP-I	---	---
C59	PEG_RX2_-	PEG Lane 2 Receive -	DP-I	---	---
C60	GND	Power Ground	PWR GND	---	---
C61	PEG_RX3_+	PEG Lane 3 Receive +	DP-I	---	---
C62	PEG_RX3_-	PEG Lane 3 Receive -	DP-I	---	---
C63	TSN0_RX_+	Not Connected	NC	---	Untested option for Time Sensitive Networking SGMII interface.
C64	TSN0_RX_+	Not Connected	NC	---	Untested option for Time Sensitive Networking SGMII interface.

Pin	Signal	Description	Type	Termination	Comment
C65	PEG_RX4_+	PEG Lane 4 Receive +	DP-I	---	---
C66	PEG_RX4_-	PEG Lane 4 Receive -	DP-I	---	---
C67	RAPID_SHUTDOWN	Rapid Shutdown Trigger Input	I-3.3	PD 100K	---
C68	PEG_RX5_+	PEG Lane 5 Receive +	DP-I	---	---
C69	PEG_RX5_-	PEG Lane 5 Receive -	DP-I	---	---
C70	GND	Power Ground	PWR GND	---	---
C71	PEG_RX6_+	PEG Lane 6 Receive +	DP-I	---	---
C72	PEG_RX6_-	PEG Lane 6 Receive -	DP-I	---	---
C73	GND	Power Ground	PWR GND	---	---
C74	PEG_RX7_+	PEG Lane 7 Receive +	DP-I	---	---
C75	PEG_RX7_-	PEG Lane 7 Receive -	DP-I	---	---
C76	GND	Power Ground	PWR GND	---	---
C77	GMII_MDIO	Not Connected	NC	---	Untested option for Time Sensitive Networking SGMII interface.
C78	PEG_RX8_+	PEG Lane 8 Receive +	DP-I	---	---
C79	PEG_RX8_-	PEG Lane 8 Receive -	DP-I	---	---
C80	GND	Power Ground	PWR GND	---	---
C81	PEG_RX9_+	PEG Lane 9 Receive +	DP-I	---	---
C82	PEG_RX9_-	PEG Lane 9 Receive -	DP-I	---	---
C83	GMII_MDC	Not Connected	NC	---	Untested option for Time Sensitive Networking SGMII interface.
C84	GND	Power Ground	PWR GND	---	---
C85	PEG_RX10_+	PEG Lane 10 Receive +	DP-I	---	---
C86	PEG_RX10_-	PEG Lane 10 Receive -	DP-I	---	---
C87	GND	Power Ground	PWR GND	---	---
C88	PEG_RX11_+	PEG Lane 11 Receive +	DP-I	---	---
C89	PEG_RX11_-	PEG Lane 11 Receive -	DP-I	---	---
C90	GND	Power Ground	PWR GND	---	---
C91	PEG_RX12_+	PEG Lane 12 Receive +	DP-I	---	---
C92	PEG_RX12_-	PEG Lane 12 Receive -	DP-I	---	---
C93	GND	Power Ground	PWR GND	---	---
C94	PEG_RX13_+	PEG Lane 13 Receive +	DP-I	---	---
C95	PEG_RX13_-	PEG Lane 13 Receive -	DP-I	---	---
C96	GND	Power Ground	PWR GND	---	---
C97	NC	Reserved for future use	NC	RSVD	---
C98	PEG_RX14+	PEG Lane 14 Receive +	DP-I	---	---
C99	PEG_RX14-	PEG Lane 14 Receive -	DP-I	---	---
C100	GND	Power Ground	PWR GND	---	---
C101	PEG_RX15_+	PEG Lane 15 Receive +	DP-I	---	---
C102	PEG_RX15_-	PEG Lane 15 Receive -	DP-I	---	---
C103	GND	Power Ground	PWR GND	---	---
C104	V_IN_VAR	Main Input Voltage (4.75V-20V)	PWR 4.75-20V	---	---

Pin	Signal	Description	Type	Termination	Comment
C105	V_IN_VAR	Main Input Voltage (4.75V-20V)	PWR 4.75-20V	---	---
C106	V_IN_VAR	Main Input Voltage (4.75V-20V)	PWR 4.75-20V	---	---
C107	V_IN_VAR	Main Input Voltage (4.75V-20V)	PWR 4.75-20V	---	---
C108	V_IN_VAR	Main Input Voltage (4.75V-20V)	PWR 4.75-20V	---	---
C109	V_IN_VAR	Main Input Voltage (4.75V-20V)	PWR 4.75-20V	---	---
C110	GND	Power Ground	PWR GND	---	---

5.6. Connector (X1B) Row D1 - D110

Table 41: Connector (X1B) Row D1 to D110 Pin Assignment

Pin	Signal	Description	Type	Termination	Comment
D1	GND	Power Ground	PWR GND	---	---
D2	GND	Power Ground	PWR GND	---	---
D3	USB_SSTX0_-	USB Super Speed Transmit 0 -	DP-O	---	---
D4	USB_SSTX0_+	USB Super Speed Transmit 0 +	DP-O	---	---
D5	GND	Power Ground	PWR GND	---	---
D6	USB_SSTX1_-	USB Super Speed Transmit 1 -	DP-O	---	---
D7	USB_SSTX1_+	USB Super Speed Transmit 1 +	DP-O	---	---
D8	GND	Power Ground	PWR GND	---	---
D9	USB_SSTX2_-	USB Super Speed Transmit 2 -	DP-O	---	---
D10	USB_SSTX2_+	USB Super Speed Transmit 2 +	DP-O	---	---
D11	GND	Power Ground	PWR GND	---	---
D12	USB_SSTX3_-	USB Super Speed Transmit 3 -	DP-O	---	---
D13	USB_SSTX3_+	USB Super Speed Transmit 3 +	DP-O	---	---
D14	GND	Power Ground	PWR GND	---	---
D15	DDI1_DDCCLK_AUX_+	DDI1 CTRLCLK/AUX+	I/O-3.3	PD 100k	---
D16	DDI1_DDCDATA_AUX_-	DDI1 CTRLDATA/AUX-	I/O-3.3	PU 100k 3.3V (S0)	---
D17	USB4_PD_I2C_ALERT#	Reserved for future use	NC	---	---
D18	PMC_ALERT#	Reserved for future use	NC	---	---
D19	PCIE_TX6_+	PCI Express Lane 6 Transmit +	DP-O	---	---
D20	PCIE_TX6_-	PCI Express Lane 6 Transmit -	DP-O	---	---
D21	GND	Power Ground	PWR GND	---	---
D22	PCIE_TX7_+	PCI Express Lane 7 Transmit +	DP-O	---	---
D23	PCIE_TX7_-	PCI Express Lane 7 Transmit -	DP-O	---	---
D24	NC	Reserved for future use	NC	---	RSVD
D25	EDP2_VDD_EN	Not connected on variants without second eDP port (option for second eDP port – VDD enable)	NC (IO-3.3V)	n/a (PD 100k)	Optional on variants with two eDP ports.
D26	DDI1_PAIR0_+	DDI1 Pair 0 +	DP-O	---	---
D27	DDI1_PAIR0_-	DDI1 Pair 0 -	DP-O	---	---
D28	EDP2_BKLT_EN	Not connected on variants without second eDP port (option for second eDP port – backlight enable)	NC (IO-3.3V)	n/a (PD 100k)	Optional on variants with two eDP ports.
D29	DDI1_PAIR1_+	DDI1 Pair 1 +	DP-O	---	---
D30	DDI1_PAIR1_-	DDI1 Pair 1 -	DP-O	---	---
D31	GND	Power Ground	PWR GND	---	---

Pin	Signal	Description	Type	Termination	Comment
D32	DDI1_PAIR2+	DDI1 Pair 2 +	DP-O	---	---
D33	DDI1_PAIR2-	DDI1 Pair 2 -	DP-O	---	---
D34	DDI1_DDC_AUX_SEL	DDI1 DDC/AUX Select	I-3.3	PD 1M	---
D35	DDI2_TBT_LSX1_RXD	Not connected	NC	---	Untested option for possible Thunderbolt implementation.
D36	DDI1_PAIR3_+	DDI1 Pair 3 +	DP-O	---	---
D37	DDI1_PAIR3_-	DDI1 Pair 3 -	DP-O	---	---
D38	EDP2_HPD	Second eDP port HPD signal	I-3.3V	PD 100k	All variants, functional only for COMe 3.1 carrier; COMe 3.0 uses pin as GND.
D39	DDI2_PAIR0_+	DDI2 Pair 0 +	DP-O	---	---
D40	DDI2_PAIR0_-	DDI2 Pair 0 -	DP-O	---	---
D41	GND	Power Ground	PWR GND	---	---
D42	DDI2_PAIR1_+	DDI2 Pair 1 +	DP-O	---	---
D43	DDI2_PAIR1_-	DDI2 Pair 1 -	DP-O	---	---
D44	DDI2_HPD	DDI2 Hotplug Detect	I-3.3	PD 100k	---
D45	EDP2_BKLT_CTRL	Not connected on variants without second eDP port (option for second eDP port – backlight enable)	NC (IO-3.3V)	n/a (PD 100k)	Optional on variants with two eDP ports.
D46	DDI2_PAIR2_+	DDI2 Pair 2 +	DP-O	---	---
D47	DDI2_PAIR2_-	DDI2 Pair 2 -	DP-O	---	---
D48	NC	Reserved for future use	NC	---	RSVD
D49	DDI2_PAIR3_+	DDI2 Pair 3 +	DP-O	---	---
D50	DDI2_PAIR3_-	DDI2 Pair 3 -	DP-O	---	---
D51	GND	Power Ground	PWR GND	---	---
D52	PEG_TX0_+	PEG Lane 0 Transmit +	DP-O	---	---
D53	PEG_TX0_-	PEG Lane 0 Transmit -	DP-O	---	---
D54	PEG_LANE_RV#	PEG Port Lane Order Reversal Input	I-3.3	PU 10k 3.3V (S5)	---
D55	PEG_TX1_+	PEG Lane 1 Transmit +	DP-O	---	---
D56	PEG_TX1_-	PEG Lane 1 Transmit -	DP-O	---	---
D57	GND	GND for type 6 module	PWR	---	---
D58	PEG_TX2_+	PEG Lane 2 Transmit +	DP-O	---	---
D59	PEG_TX2_-	PEG Lane 2 Transmit -	DP-O	---	---
D60	GND	Power Ground	PWR GND	---	---
D61	PEG_TX3_+	PEG Lane 3 Transmit +	DP-O	---	---
D62	PEG_TX3_-	PEG Lane 3 Transmit -	DP-O	---	---
D63	TSN0_TX_+	Not Connected	NC	---	Untested option for Time Sensitive Networking SGMII interface.

Pin	Signal	Description	Type	Termination	Comment
D64	TSN0_TX_-	Not Connected	NC	---	Untested option for Time Sensitive Networking SGMII interface.
D65	PEG_TX4_+	PEG Lane 4 Transmit +	DP-O	---	---
D66	PEG_TX4_-	PEG Lane 4 Transmit -	DP-O	---	---
D67	GND	Power Ground	PWR GND	---	---
D68	PEG_TX5_+	PEG Lane 5 Transmit +	DP-O	---	---
D69	PEG_TX5_-	PEG Lane 5 Transmit -	DP-O	---	---
D70	GND	Power Ground	PWR GND	---	---
D71	PEG_TX6_+	PEG Lane 6 Transmit +	DP-O	---	---
D72	PEG_TX6_-	PEG Lane 6 Transmit -	DP-O	---	---
D73	GND	Power Ground	PWR GND	---	---
D74	PEG_TX7_+	PEG Lane 7 Transmit +	DP-O	---	---
D75	PEG_TX7_-	PEG Lane 7 Transmit -	DP-O	---	---
D76	GND	Power Ground	PWR GND	---	---
D77	RGMII_RESET#	Not Connected	NC	---	Untested option for Time Sensitive Networking SGMII interface.
D78	PEG_TX8_+	PEG Lane 8 Transmit +	DP-O	---	---
D79	PEG_TX8_-	PEG Lane 8 Transmit -	DP-O	---	---
D80	GND	Power Ground	PWR GND	---	---
D81	PEG_TX9_+	PEG Lane 9 Transmit +	DP-O	---	---
D82	PEG_TX9_-	PEG Lane 9 Transmit -	DP-O	---	---
D83	RGMII_INT#	Not Connected	NC	---	Untested option for Time Sensitive Networking SGMII interface.
D84	GND	Power Ground	PWR GND	---	---
D85	PEG_TX10_+	PEG Lane 10 Transmit +	DP-O	---	---
D86	PEG_TX10_-	PEG Lane 10 Transmit -	DP-O	---	---
D87	GND	Power Ground	PWR GND	---	---
D88	PEG_TX11_+	PEG Lane 11 Transmit +	DP-O	---	---
D89	PEG_TX11_-	PEG Lane 11 Transmit -	DP-O	---	---
D90	GND	Power Ground	PWR GND	---	---
D91	PEG_TX12_+	PEG Lane 12 Transmit +	DP-O	---	---
D92	PEG_TX12_-	PEG Lane 12 Transmit -	DP-O	---	---
D93	GND	Power Ground	PWR GND	---	---
D94	PEG_TX13_+	PEG Lane 13 Transmit +	DP-O	---	---
D95	PEG_TX13_-	PEG Lane 13 Transmit -	DP-O	---	---

Pin	Signal	Description	Type	Termination	Comment
D96	GND	Power Ground	PWR GND	---	---
D97	NC	Reserved for future use	NC	---	RSVD
D98	PEG_TX14_+	PEG Lane 14 Transmit +	DP-O	---	---
D99	PEG_TX14_-	PEG Lane 14 Transmit -	DP-O	---	---
D100	GND	Power Ground	PWR GND	---	---
D101	PEG_TX15_+	PEG Lane 15 Transmit +	DP-O	---	---
D102	PEG_TX15_-	PEG Lane 15 Transmit -	DP-O	---	---
D103	GND	Power Ground	PWR GND	---	---
D104	V_IN_VAR	Main Input Voltage (4.75V-20V)	PWR 4.75-20V	---	---
D105	V_IN_VAR	Main Input Voltage (4.75V-20V)	PWR 4.75-20V	---	---
D106	V_IN_VAR	Main Input Voltage (4.75V-20V)	PWR 4.75-20V	---	---
D107	V_IN_VAR	Main Input Voltage (4.75V-20V)	PWR 4.75-20V	---	---
D108	V_IN_VAR	Main Input Voltage (4.75V-20V)	PWR 4.75-20V	---	---
D109	V_IN_VAR	Main Input Voltage (4.75V-20V)	PWR 4.75-20V	---	---
D110	GND	Power Ground	PWR GND	---	---

6/ UEFI BIOS

6.1. Starting the uEFI BIOS

The COM-bTL6 uses a Kontron-customized, pre-installed and configured version of AMI Aptio V BIOS ® based on the Unified Extensible Firmware Interface (uEFI) specification and the Intel® Platform Innovation Framework for EFI. The uEFI BIOS provides a variety of new and enhanced functions specifically tailored to the hardware features of the COM-bTL6.

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

Register for Kontron's Customer Section to get access to BIOS downloads and 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.

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 Chapter 6.4.4: Security Setup Menu , press <RETURN>, and proceed with step 5.
5. The Setup menu appears.

6.2. Navigating the uEFI BIOS

The COM-bTL6 uEFI BIOS Setup program uses a hot key navigation system. The hot key legend bar is located at the bottom of the BIOS setup screens. The following table provides a list of navigation hot keys available in the legend bar.

Table 42: Navigation Hot Keys Available in the Legend Bar

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

Sub-screen	Description
<ESC>	<ESC> key exits a major Setup menu and enters the Exit Setup menu. Pressing the <ESC> key in a sub-menu displays the next higher menu level
<RETURN>	<RETURN> key executes a command or selects a submenu

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

Each Setup menu provides two main frames. The left frame displays all available functions and configurable functions are displayed in blue. Functions displayed in grey provide information about the status or the operational configuration.

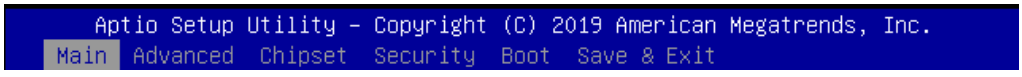
6.3. Getting Help

The right frame displays a help window. The help window provides an explanation of the respective function.

6.4. Setup Menus

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

Figure 12: Setup Menu Selection Bar



The Setup menus available for the COMe-bTL6 are:

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

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

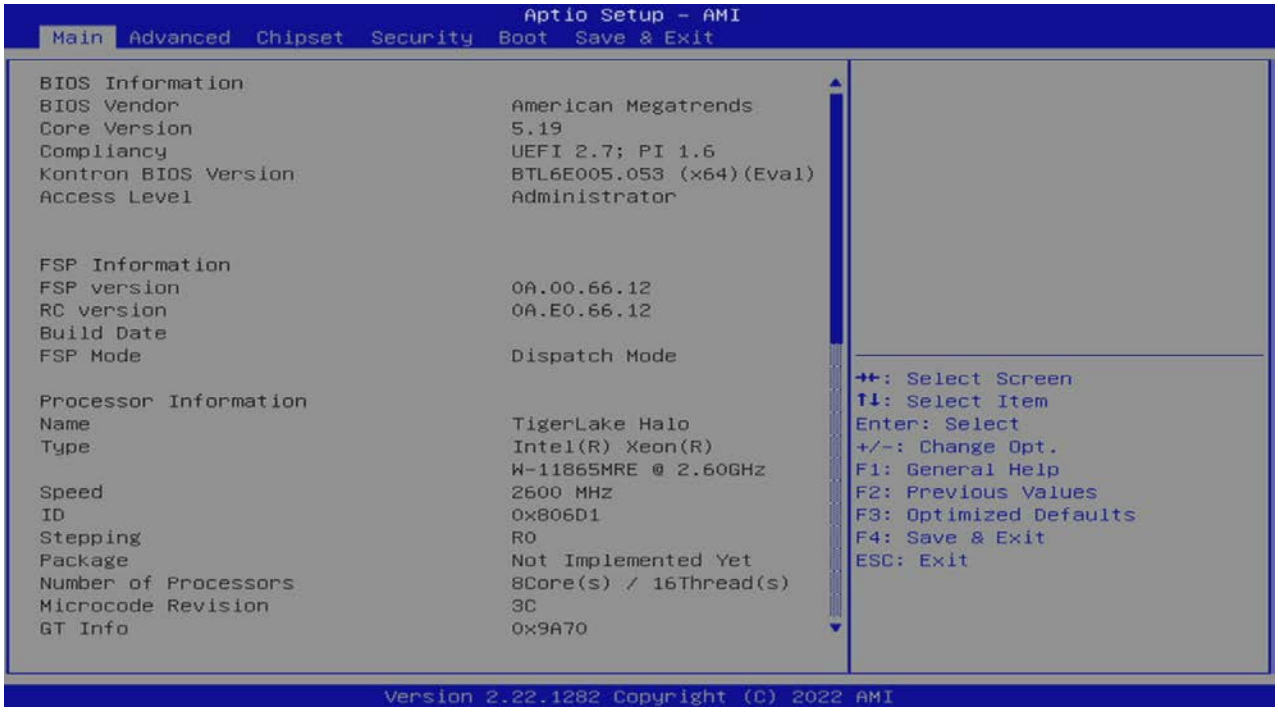
Each Setup menu provides two main frames. The left frame displays all available functions. Configurable functions are displayed in blue. Functions displayed in grey provide information about the status or the operational configuration.

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

6.4.1. Main Setup Menu

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

Figure 13: Main Setup Menu



The following table shows the Main Menu sub-screens and functions and describes the content. Default options are displayed **bold**.

Table 43: Main Setup Menu Sub-screens

Sub-Screen	Description
BIOS Information	Read only field BIOS Information: BIOS Vendor, Core Version, Compliancy, Kontron BIOS Version and Access Level
FSP Information	Read only field FSP Information: FSP Version, RC Version, Build Date and FSP Mode.
Processor Information	Read only field Processor Information: Name, Type, Speed, ID, Stepping, Package, Number of Processors, Microcode Revision, GT Info, eDRAM Size IGFX GOP Version, PCIe GEN4 Dekel FW Version, Total Memory and Memory Speed.
PCH Information	Read only field PCH Information: Name, PCH SKU, Stepping, Chipset Init Base Revision, Chipset Init OEM Revision, Package, TXT Capability, Production Type, ME FW Version, ME Firmware SKU, PMC FW Version
System Language	[**English**]
Platform Information	Read only field Module Information: Product Name, Revision, Serial # ,MAC Address, Boot Counter, and CPLD Rev.

Sub-Screen	Description
	Additional information for MAC Address The MAC address entry is the value used by the Ethernet controller and may contain the entry 'Inactive' - Ethernet chip is inactive. Activate - Ethernet chip: Advanced > Network Stack Configuration > Network Stack > UEFI Network Stack > Enable
System Date	Displays the system date [Day mm/dd/yyyy]
System Time	Displays the system time [hh:mm:ss]

6.4.2. Advanced Setup Menu

The Advanced Setup menu provides sub-screens and second level sub-screens with functions for advanced configuration.

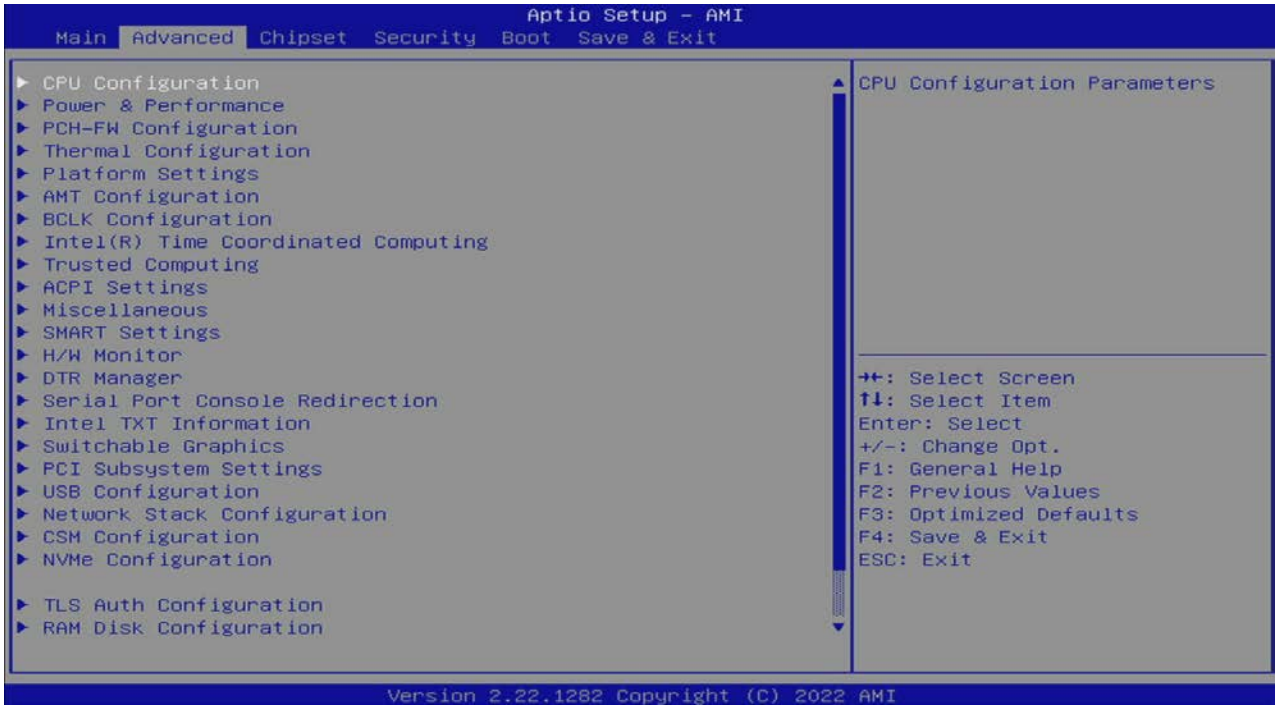
NOTICE

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

NOTICE

UART0 uses a PCI root function and would cause all serial interfaces to disappear if physically disabled. To avoid this and other issues, the UARTS on this system may not be disabled.

Figure 14: Advanced Setup Menu Initial Screen



The following table shows the Advanced sub-screen and describes the function. Default settings are in **bold**.

Table 44: Advanced Setup Menu Sub-screens and Functions

Sub-Screen	Function	Second level Sub-Screen/Description
CPU Configuration>	Read only field CPU Information : Type, ID, Speed, L1 Data Cache, L1 Instruction Cache, L2 Cache, L3 Cache, L4 Cache, VMX, SMX/TXT	
	C6DRAM	Moving DRAM contents to PRM memory when CPU is in C6 state [**Enabled**, Disabled]
	CPU Flex Ratio Override	CPU Flex Ratio Programming [Enabled, **Disabled**]
	CPU Flex Settings	[19]
	Intel (VMX) Virtualization Technology	When enabled VMM can utilize the additional hardware capabilities provided by Vanderpool Technology [**Enabled**, Disabled]
	Active Processor Cores	Number of cores to enable in each processor package [**All**, 1, 2, 3, 4, 5, 6, 7]

Sub-Screen	Function	Second level Sub-Screen/Description	
CPU Configuration>	Hyper Threading	[**Enabled**, Disabled]	
	BIST	[Enabled, **Disabled**]	
	AES	[**Enabled,** Disabled]	
	RaceConditionResponse Policy	[Enabled, **Disabled**]	
Power & Performance>	CPU Power Management Control>	Boot performance mode	[Max Battery**,** Max Non-Turbo Performance, **Turbo Performance**]
		Intel® SpeedStep™	Allows more than two frequency ranges to be supported. [**Enabled,** Disabled]
		Intel® Speed Shift Technology	Enable exposes CPPC v2 interface to allow for hardware controlled p-states. [**Enabled,** Disabled]
		Per Core P State OS control mode	Disable set Bit 31 =1 command 0x06. When set the highest core request is used for all other core requests. [**Enabled**, Disabled]
		HwP Autonomous Per Core P State	Disable requests the same value for all cores all the time. [**Enabled**, Disabled]
		HwP Autonomous EPP Grouping	Disable will not necessarily request same values for all cores with same EPP. [**Enabled**, Disabled]
		EPB Override over PECI	Enable by sending pcode command 0x2b, subcommand 0x3 to 1. This allows OOB EPB PECI override control. [Enabled, **Disabled**]
		HwP Fast MSR Support	Support for IA32_HWP_REQUEST MSR. [**Enabled**, Disabled]
		Turbo Mode	Note: Requires EMTTM to be enabled. AUTO means enabled. [**Enabled**, Disabled]
		View/Configure Turbo Options>	Read only field Current turbo settings: Max Turbo Power Limit, Min Turbo Power Limit, Package TDP Limit, Power Limit 1 / 2 and 1 to 6 Core Turbo Ratio Limit Ratio. (TRLR).
			Energy Efficient P-State: [**Enabled**, Disabled]
			Package Power Limit MSR Lock: Enable to lock. A reset is required to unlock the register. [Enabled, **Disabled**]
			1-Core Turbo Ratio Limit Ratio (TRLR) Override [47]

Sub-Screen	Function	Second level Sub-Screen/Description		
Power & Performance>	CPU Power Management Control>	View/Configure Turbo Options>	2-Core Turbo Ratio Limit Ratio (TRLR) Override [46]	
			3-Core Turbo Ratio Limit Ratio (TRLR) Override [45]	
			4-Core Turbo Ratio Limit Ratio (TRLR) Override [45]	
			5-Core Turbo Ratio Limit Ratio (TRLR) Override [44]	
			6-Core Turbo Ratio Limit Ratio (TRLR) Override [43]	
			7-Core Turbo Ratio Limit Ratio (TRLR) Override [43]	
			8-Core Turbo Ratio Limit Ratio (TRLR) Override [42]	
			Energy Efficient Turbo	Lowers turbo frequency to increase efficiency. [**Enabled**, Disabled]
		Config TDP Configurations>	Enable Configurable TDP	[Applies to non-cTDP, **Applies to cTDP**]
			Configurable TDP Boot Mode	[**Nominal**, Down, Deactivate]
			Configurable TDP Lock	[Enabled, **Disabled**]
			ConfigTDP levels	2
			ConfigTDP Turbo Activation Ratio	25
			Power Limit 1	45.0W (MSR:45.0)
			Power Limit 2	109.0W (MSR:109.0)
			Customer Settings Nominal	
			ConfigTDP Nominal	Ratio:26 TAR:25 PL1: 13.0W
			Power Limit 1	0
			Power Limit 2	0
			Power Limit 1 Time Window	[0, 1 …96, 112, 128]
			ConfigTDP Turbo Activation Ratio	0
			Customer Settings Down	
			ConfigTDP Nominal	Ratio:21 TAR:20 PL1: 3.0W
			Power Limit 1	0
			Power Limit 2	0
			Power Limit 1	[0, 1 …96, 112, 128]

Sub-Screen	Function	Second level Sub-Screen/Description		
Power & Performance>	CPU Power Management Control>	Config TDP Configurations>	Time Window	
			ConfigTDP Turbo Activation Ratio	0
		Platform PL1	PL1 value defines the CPU's average TDP mode consumption power; when disabled CPU uses default PL1 values. [Enabled, **Disabled**]	
		Platform PL2	PL2 value defines the CPU's average TDP mode consumption power; when disabled CPU uses default PL2 values. [Enabled, **Disabled**]	
		Platform PL4 Override	PL4 override when disabled CPU uses default PL4 values. [Enabled, **Disabled**]	
		C States	CPU power management. Allows CPU to enter C States when not 100% utilized. [**Enabled,** Disabled]	
		Package C State List	Maximum C State limit setting, where AUTO initializes to deepest available package C State limit. [**Auto**, CPU Default, C0/C1, C2,……C10]	
	GT Power Management Control>	RC6 (Render Standby)	Check to enable render standby support. [**Enabled**, Disabled]	
		Maximum GT frequency	Values beyond the range clipped to min/max supported by SKU. [**Default Max Frequency,** 100 MHz, 150 MHz, …1200 MHz]	
		Prevent Turbo on GT frequency	Enable to disable the Turbo GT when disabled GT frequency is not limited. [Enabled, **Disabled**]	
PCH-FW Configuration>	Read only field ME Firmware Version, ME Firmware Mode, ME Firmware SKU, ME Firmware Status 1, ME Firmware Status 2			
	ME State	[**Enabled**, Disabled]		
	Firmware Update Configuration>	Me FW Image Re-Flash	[Enabled, **Disabled**]	
		FW Update	[**Enabled**, Disabled]	
	PTT Configuration>	PTT Capability/State	1/0	
		TPM Device Selection	[**dTPM**, PTT]	
	Extended CSME Measurement to TPM-PCT	[Disabled]		
Thermal Configuration>	Use Generic Thermal Functions	[**Enabled**, Disabled]		
	CPU Thermal Configuration>	DTS SMM	Disabled: uses HWM reported temperature values Enabled: uses DTS SMM mechanism to obtain CPU temperature values	

Sub-Screen	Function	Second level Sub-Screen/Description	
Thermal Configuration>	CPU Thermal Configuration>	DTS SMM	Out of spec: uses HWM and DTS SMM [Enabled, **Disabled**, Critical Temp Reporting (Out of Spec)]
		TCC Activation Offset	Sets temperature at which TCC must be activated (range: 0 to 60). [0]
		Disable PROCHOT# Output	[**Enabled**, Disabled]
	Platform Thermal Configuration>	Critical Trip Point	The point at which the OS begins to shut the system off. [**119 C (POR),** 130 C,...15 C]
		Passive Trip Point	The point at which the OS begins to throttling the processor. [**95 C**, 119 C (POR), ...15 C, Disabled]
		Passive TC1 Value	TC1 value for ACPI passive cooling formula (range: 1 to 16). [1]
		Passive TC2 Value	TC2 value for ACPI passive cooling formula (range: 1 to 16) . [5]
		Passive TSP Value	Sets TSP value for ACPI passive cooling formula (range: 2 to 32). Represent in tenths of second how often the temperature is read when passive cooling enabled. [10]
		Passive Trip Points	[Enabled, **Disabled**]
		Critical Trip Points	[**Enabled**, Disabled]
		Boot DTS Read	Read PCH, CPU DTS Temperature and Publish via SMBIOS table [Enabled, **Disabled**]
Platform Settings>	Firmware Configuration	[Ignore Policy Update, Production, **Test**]	
	PS2 Keyboard and Mouse	[**Enabled**, Disabled]	
	Power Loss Notification Feature	[Enabled, **Disabled**]	
	Intel Trusted Device Setup Boot	[Enabled, **Disabled**]	
	PMC Fast Boot	[Enabled, **Disabled**]	
AMT Configuration>	USB Provisioning of AMT	[Enabled, **Disabled**]	
	MAC Pass Through	[Enabled, **Disabled**]	
	CIRA Configuration>	Activate Remote Assistance Process	Trigger CIRA boot. NOTE: First access must be activated from MEBX setup. [Enabled, **Disabled**]
		CIRA Timeout	0
	ASF Configuration>	PET progress	[**Enabled**, Disabled]

Sub-Screen	Function	Second level Sub-Screen/Description	
AMT Configuration>	ASF Configuration>	Watchdog	[Enabled, **Disabled**]
		OS Timer	0
		BIOS Timer	0
		ASF Sensors Table	Adds ASF sensor table into ASF ACPI Table. [Enabled, **Disabled**]
	Secure Erase Configuration>	Secure Erase Mode	Simulate: Performs SE flow without erasing SSD Real: Erases SSD [**Simulate**, Real]
		Force Secure Erase	Force Secure Erase on next boot. [Enabled, **Disabled**]
	OEM Flag Settings>	MEBx hotkey Pressed	OEM Flag Bit 1 enables automatics MEBx hotkey. [Enabled, **Disabled**]
		MEBx Selection Screen	OEM Flag Bit 2 enables MEBx selection screen with two options: (1) To enter ME Configuration Screen (2) Initiate remote connection. Note: Network access must be activated from MEBx setup for this screen to be displayed. [Enabled, **Disabled**]
		Hide Unconfigure ME Confirmation Prompt>	OEM Flag Bit 6: Hides the prompt when attempting ME unconfiguration. [Enabled, **Disabled**]
		MEBx OEM D ebug Menu Enable	OEM flag Bit 14 [Enabled, **Disabled**]
		Unconfigure ME	OEM Flag Bit 15: Unconfigure ME with resetting MEBx password to default [Enabled, **Disabled**]
	MEBx Resolution Settings>	Non-UI Mode Resolution	[**Auto**, 80x25, 100x31]
		UI Mode Resolution	[**Auto**, 80x25, 100x31]
		Graphics Mode Resolution	[**Auto**, 640x480, 800x600, 1024x768]
BCLK Configuration>	BCLK Source Config	Selects BCLK configuraton: CPU7pcode controlled BCLK or PC/CSME controlled BCLK. Note: the POR for TGL is CPU BCLK [**CPU BCLK**, PCH BCLK]	
	CPU-BCLK Clock Settings		
	BCLK RFI Frequency SAGV Low	Frequency in 10 KHz increments (range: 0 MHz to 98-100 MHz) 0	
	BCLK RFI Frequency SAGV Mid	Frequency in 10 KHz increments (range: 0 MHz to 98-100 MHz) 0	
	BCLK RFI Frequency SAGV High	Frequency in 10 KHz increments (range: 0 MHz to 98-100 MHz) 0	
	BCLK RFI Frequency SAGV Max	Frequency in 10 KHz increments (range: 0 MHz to 98-100 MHz)	

Sub-Screen	Function	Second level Sub-Screen/Description	
BCLK Configuration>		0	
	BCLK Spread	When enabled BCKL frequency runs at a non-configurable fixed spread percentage. [**Enabled**, Disabled]	
Intel® Time Coordinated Computing>	#AC Split Lock	Enable: asserts #AC when atomic operation has operand crossing two cache lines [Enabled, **Disabled**]	
	IFU State	Enable: instructions prefetch to the cache [Enabled, **Disabled**]	
	Software SRAM	Enable: allocated one way of LLC. If cache configuration sub-region is available, it allocates based on sub-region. Enabled, **Disabled**]	
	Data Streams Optimizer	Enable: utilizes DSO sub-region to tune system. [Enabled, **Disabled**]	
	Error Log	Enable: logs errors related to Intel® TCC and saves to memory. [**Enabled**, Disabled]	
	Intel® TCC Authentication Menu>	Intel® TCC Authentication	Determines key to be used, non-OEM enrolled key can be added by user. [Disabled, Non-OEM Enrolled Key, **OEM Enrolled Key**]
	Intel® TCC Mode	Enable modifies setting to improve real-time performance. [Enabled, **Disabled**]	
	Intel® TCC Mode Affected Settings		
	IO Fabric Low Latency	Turns of some power management in PCH IO fabrics. S3 state is not supported. [Enabled, **Disabled**]	
	GT CLOS	Enable reduces Gfx LCC allocation to minimize impact of Gfx workload on LLC. [Enabled, **Disabled**]	
	OPIO Recentering	Improves PCIe latency. [**Enabled**, Disabled]	
	C States>	Enabling allows CPU to enter c states when it is no 100% utilized. [**Enabled**, Disabled]	
	Intel® Speed Shift Technology>	Enabling exposes CPPC V2 interface to allow for hardware controlled P-states. [**Enabled**, Disabled**]**	
	Intel® SpeedStep ™>	Enabling exposes CPPC V2 interface to allow for hardware controlled P-states. [**Enabled,** Disabled**]**	
	Hyper-Threading>	Enables or disables the Hyper-Threading Technology. [**Enabled**, Disabled**]**	
	ACPI D3Cold Support>	ACPI D3Cold support to be executed on D3 entry and exit. [Enabled**, Disabled**]	
	Low Power S0 Idle Capability>	Chooses the power saving states the system uses in ACPI OS. ACPI Energy save option: S3/S4 (Disabled) und S0iX (Enabled). [Enabled**, Disabled**]	
	WRC Feature>	Enable supports IO devices allocated onto the ring and into LLC.	

Sub-Screen	Function	Second level Sub-Screen/Description		
Intel® Time Coordinated Computing>		[Enabled, **Disabled**]		
	VCRt mapping to PEG	Enables or disables VCRt mapping to PRG. [Enabled, **Disabled**]		
	Page Close Idle Timeout>	Page Close Idle Timeout Control		
	Power Down Mode>	CKE Power Down Mode Control		
	RC6 (Render Standby)	[**Enabled,** Disabled]		
	DMI Link ASPM Control>	See Chipset> PCI Express Configuration		
	PCI Express Clock Gating>	See Chipset> PCI Express Configuration		
	Legacy IO Low Latency>	Enable: sets low latency of legacy IO [Enabled, **Disabled**]		
	CPU PCI Express Configuration>	PCI Express Root Port 1, 2, 3, 4>	ASPM	[**Disabled**, L1]
			L1 Substates	[Disabled , L1.1, **L1.1 & L1.2**]
	PCH PCI Express Configuration>	PCI Express Root Port 1, 2, 3, 4 >	ASPM	[**Disabled**, L0s, L1, L0sL1, Auto]
Trusted Computing>	Read only Field TPM 2.0 Device Found, Firmware Version and Vendor.			
	Security Device Support	BIOS support for security devices. OS will not show security device. TCG EFI protocol and INT1A interface not available. [**Enabled,** Disabled]		
	Active PCR Banks	SHA256		
	Available PCR Banks	SHA256		
	SHA256 PCR Bank	Enable or disable SHA256 PCR bank [**Enabled**, Disabled]		
	Pending Operation	Schedule an operation for your security device. Note: reboots during restart to change state of security device. [**None,** TPM Clear]		
	Platform Hierarchy	[**Enabled,** Disabled]		
	Storage Hierarchy	[**Enabled,** Disabled]		
	Endorsement Hierarchy	[**Enabled,** Disabled]		
	Physical Presence Spec Version	Selects OS support for PPI Spec version 1.2 or 1.3. Note: some HCK test might not support 1.3 [1.2, **1.3**]		
	TPM 2.0 Interface Type	[TIS]		
	Device Select	Auto supports both with the default set to TPM 2.0. [TPM 1.2, TPM 2.0, **Auto**]		
ACPI Settings>	ACPI Auto Configuration>	Enables or disables BIOS ACPI Auto Configuration [Enabled, **Disabled**]		
	Hibernation>	System ability to hibernate (OS/S4 sleep State). Note: This option may not be effective with some operating systems. **[Enabled**, Disabled]		
	ACPI Sleep State	Highest ACPI sleep state the system enters when the suspend button pressed. [Suspend Disabled, **S3 Suspend to RAM**]		

Sub-Screen	Function	Second level Sub-Screen/Description	
ACPI Settings>	S3 Video Repost>	[Enabled, **Disabled**]	
	Low Power S0 Idle Capability	ACPI Energy save option: S3/S4 (Disabled) und S0iX (Enabled). [Enabled, **Disabled**]	
Miscellaneous>	Generic eSPI Decode Ranges>	Generic LPC via eSPI Decode 1	Generic LPC via eSPI decode range [Enabled, **Disabled**]
	Watchdog>	Auto-reload	Automatic reload of watchdog timers on timeout [Enable, **Disabled**]
		Global Lock	Enable: watchdog registers (except WD_Kick) read only until board is reset [Enabled, **Disabled**]
		Stage 1 Mode	Select action for this watchdog phase [Enabled, **Disabled**]
	Reset Button Behavior	[**Chipset Reset**, Power Cycle]	
	I2C Speed	Speed in kHz (range: 1 kHz to 400 kHz) default 200 KHz 200	
	Onboard I2C Mode	[**Multimaster**, Busclear]	
	Manufacturing Mode	Disabled	
	BIOS Test Mode	Disabled	
	Lid Switch Mode	Show or hide inside ACPI OS [Enabled, **Disabled**]	
	Sleep Button Mode	Show or hide inside ACPI OS [Enabled, **Disabled**]	
	ACPI temperature polling	Set mode for temperature polling through OSPM [**Enabled**, Disabled]	
	TZ00 temperature polling time	Interval in seconds between two temperature measurements in ACPI thermal zone. (00, Ambient temperature) [30]	
	Create ACPI AC adaptor	Creates an ACPI AC adapter device, with virtual battery even on non-battery systems. [**Enabled**, Disable]	
	SMBus device ACPI mode	Hidden: hides SMBus device from OS Normal: visible [Hidden, **Normal**]	
	CPLD device ACPI mode	Hidden: hides CPLD device from OS Normal: visible [Hidden, **Normal**]	
	SPI lines active	Chooses whether SPI0 or GSPI0 lines are routed through COMe. [**SPI0**, GSPI0]	
	Control COMe GPIOs in BIOS	GPIO control in BIOS. If disabled GPIO are not touched by BIOS. [Enabled, **Disabled**]	
	GPIO IRQ#	Sets IRQ number to trigger by the CPLD on GPIO event. [**Disabled**, IRQ 5, IRQ 7, IRQ 12, IRQ 14, IRQ 15]	
	I2C IRQ#	Sets IRQ number to trigger by the CPLD on I2C event. [**Disabled**, IRQ 5, IRQ 7, IRQ 12, IRQ 14, IRQ 15]	

Sub-Screen	Function	Second level Sub-Screen/Description
Miscellaneous>	RTC reset control	For RTC battery-less systems a RTC reset might be needed to properly return from G3. Do not set if RTC battery is present! [Enabled, **Disabled**]
	Last system reset through	[Reset Button]
SMART Settings>	SMART Self Test	Run SMART Self Test on all HDDs during Post. [Enabled, **Disabled**]
H/W Monitor>	CPU Temperature	[99 C]
	Module Temperature	[28 C]
	CPU Fan	Displays CPU fan speed in RPM
	Fan Control	Note: Disable stops the fan totally [**Auto**, Disabled, Manual]
	Fan Pulse	Number of pulse the fan produces during one revolution [2]
	Fan Trip Point	Temperature where fan accelerates (range: 20 to 80 C) [50]
	Trip Point Speed	Fan speed at trip point in 5. Min. value is 30%. At TJmax fan always runs at 100% [50]
	Reference Temperature	Temperature source for automatic fan control [Module Temperature, **CPU Temperature**]
	External Fan	Displays External Fan speed RPM (If connected)
	Fan Control	Note: Disable stops the fan totally [**Auto**, Disabled, Manual]
	Fan Pulse	Number of pulse the fan produces during one revolution [2]
	Fan Trip Point	Temperature where fan accelerates (range: 20 to 80 C) [50]
	Trip Point Speed	Fan speed at trip point in 5. Min. value is 30%. At TJmax fan always runs at 100% [50]
	Reference Temperature	Temperature source for automatic fan control [Module Temperature, **CPU Temperature**]
	5.0V Standby	[4.57 V]
	Batt Volt at COMe Pin	[2.92 V]
	Widerrange VCC	[12.01 V]
DTR Manager>	Intel® Dynamic Temperature Range	
	CPU Temperature	Displayed in °C
	CPU T0 Temperature	Displayed in °C
	PCH Temperature	Displayed in °C
	PCH T0 Temperature	Displayed in °C
	DTR value / CPU	Displayed in °C
	DTR value / PCH	Displayed in °C

Sub-Screen	Function	Second level Sub-Screen/Description	
Serial Port Console Redirection>	COM0 Console Redirection	COM port 0 console redirection enable or disable. [Enabled, **Disabled**]	
	COM1 Console Redirection	COM port 1 console redirection enable or disable [Enabled, **Disabled**]	
	Legacy Console Redirection>	Redirection COM Port	Selects a COM port to display redirection of legacy OS and Legacy OPROM messages [**COM0 (pci Bus0, Dev30, Func0, Port1),** COM1 (pci Bus0, Dev30, Func1, Port1]
		Resolution	[**80x24,** 80x25]
	Console Redirection EMS	Serial port for Out-Of-Band Management Windows Emergency Management Services (EMS) console redirection enable or disable. [Enabled, **Disable**d]	
Intel TXT Information>	Read only field Chipset, BiosAcm. Chipset Txt, CPU Txt, Error code, Class code, Major code and Minor code		
Switch. Graphics>	SG Mode Select	Muxless	
PCI Subsystem Settings>	PCI Settings Common for all Devices		
	Re-Size BAR Support	If Resizable BAR capable PCIe deviecs are present, this option enables or disables Resizable BAR Support. [Enabled**, Disabled**]	
	BME DMA Mitigation	Re-enables Bus Master Attribute disabled during PCI enumeration for PCI Bridges after SMM Locked. [Enabled**, Disabled**]	
	Warning: Changing PCI Device(s) settings may have unwanted side effects! System may HANG! PROCEED WITH CAUTON		
USB Configuration>	Read Only Field USB Configuration: USB Module Version, USB Controllers (2 XHCIs) USB Devices (drives, keyboard, mouse, hub)		
	Legacy USB Support	Enables legacy USB support. 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	Known work around for OSes without XHCI hand-off support. The XHCI ownership change should be claimed by XHCI driver. [**Enabled,** Disabled]	
	USB Mass Storage Driver Support	[**Enabled,** Disabled]	
	USB hardware delays and time-outs:		
	USB Transfer Time-out	Time out value for Control, Bulk and Interrupt [1 sec, 5 sec, 10 sec, **20 sec**]	
	Device Reset Time-out	USB mass storage device start unit command time-out [1 sec, 5 sec, 10 sec, **20 sec**]	
	Device Power-up Delay	Maximum time device takes before reporting to the host controller properly. Auto uses default value (for a root port 100 ms and for a Hub port the delay is taken from hub descriptor).	

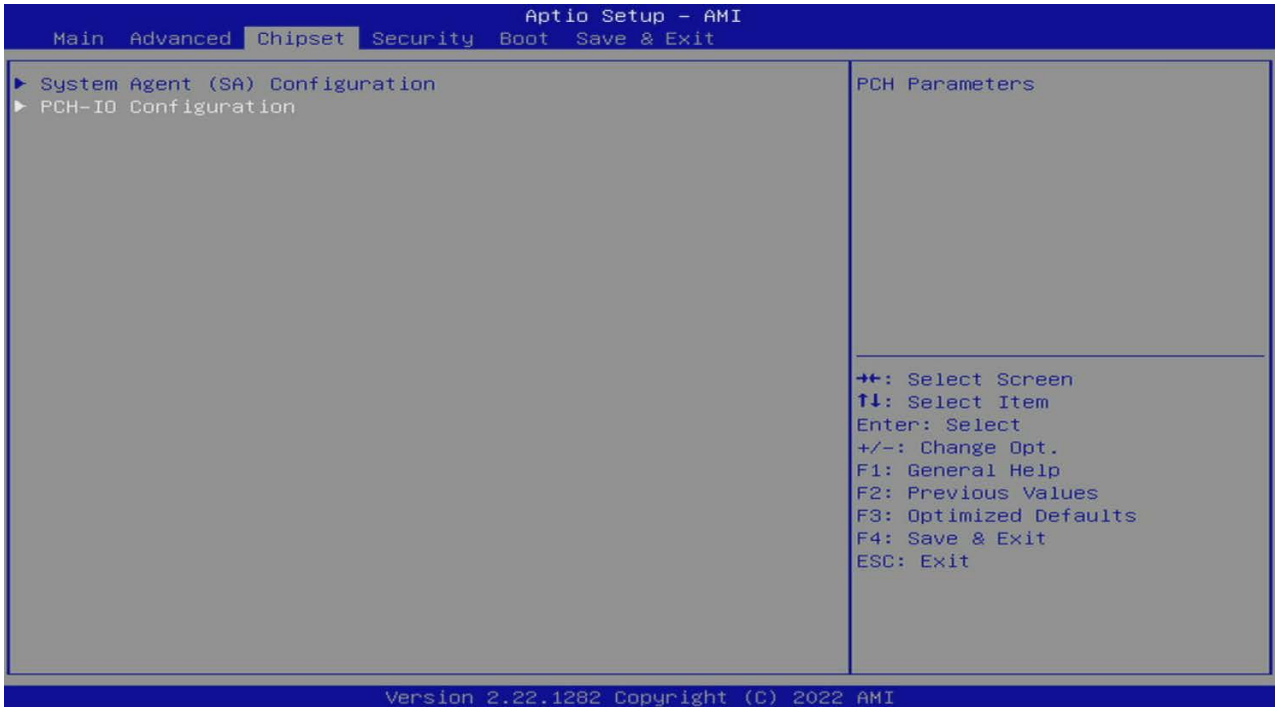
Sub-Screen	Function	Second level Sub-Screen/Description		
USB Configuration>		[**Auto**, Manual]		
	Mass Storage Devices			
	Pi-KVM CD-ROM Drive 0510	Mass storage device emulation type. Auto enumerates devices according to their media format. Optical drives are emulated as CDROM, drives with no media will be emulated according to drive type. [**Auto**, Floppy, Forced FDD, Hard Disk, CD-Rom]		
Network Stack Configuration>	Network Stack	UEFI Network Stack [Enabled, **Disabled**]		
CSM Configuration>	CSM Support	Enables or disables CSM Support. [Enabled, **Disabled**]		
NVMe Configuration>	Depends on hardware configuration.			
TLS Auth Configuration>	Server CA Configuration>	Enroll Cert>	Enroll Cert Using File	
			Cert Guide>	Input digital character
			Commit Changes and Exit	
			Discard Changes and exit	
		Delete Cert>		
	Client Cert Configuration	Read Only field		
RAM Disk Configuration>	Disk Memory Type	Specifies type of memory to use from available memory pool in system to create a disk. [**Boot Service Data**/Reserved]		
	Create Raw>	The valid RAM disk size should be multiples of the RAM disk block size. Size (Hex)		
		Create & Exit		
		Discard & Exit		
	Create from file			
	Create RAM Disk List:			
	RAM Disk 0:	[Enabled, **Disabled**]		
	Remove selected RAM disk(s)	Removes selected RAM disk(s)		
Intel® Ethernet Controller	Read only Field UEFI Drivers, Device Name, PCI Device ID, Link Status, MAC Address			
Driver Health>	Intel® Gigabit 0.9.03	Provides health status for the drivers/controllers [Healthy]		

6.4.3. Chipset Setup Menu

The Chipset Setup menu lists sub-screens and second level sub-screens of the functions supported by the PCH.

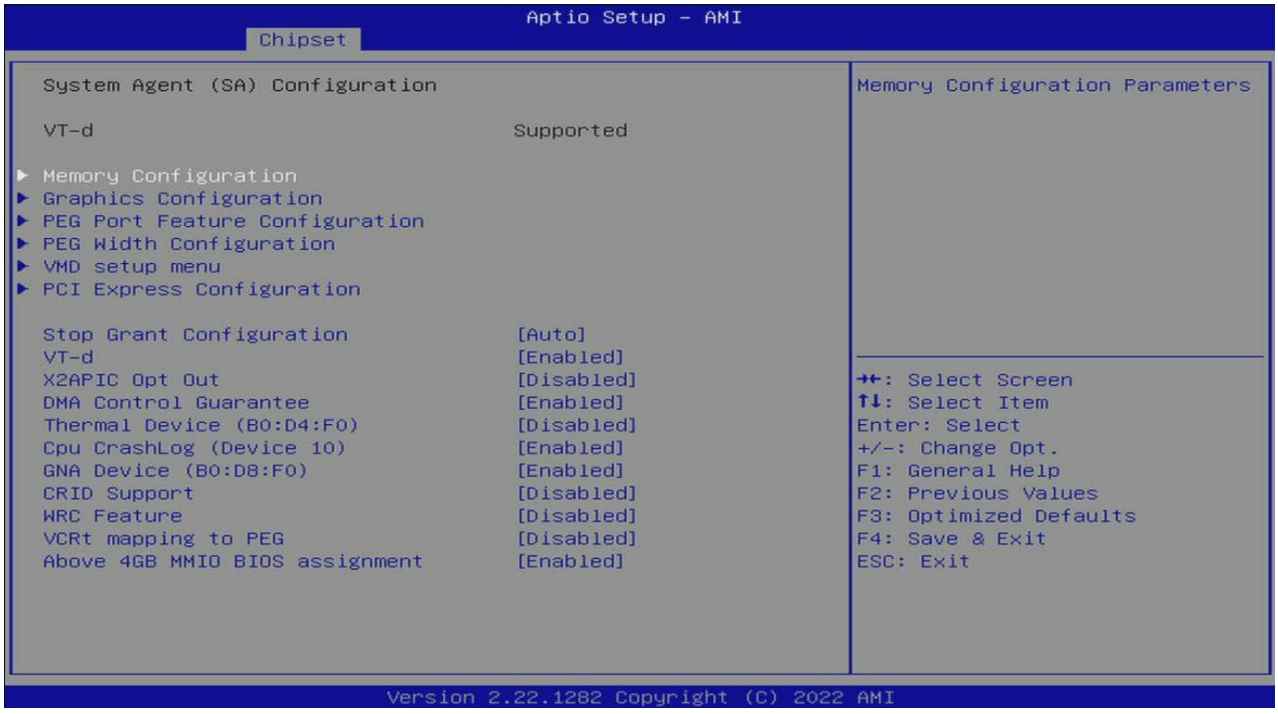
NOTICE Setting items, on this screen, to incorrect values may cause system malfunctions.

Figure 15: Chipset Setup Menu Initial Screen



6.4.3.1. Chipset System Agent (SA) Configuration Menu

Figure 16: Chipset> System Agent (SA) Configuration Setup Menu Initial Screen



The following table shows the Chipset System Agent (SA) Configuration sub-screen and describes the function. Default settings are in **bold**.

Table 45: Chipset> System Agent (SA) Configuration Menu Sub-screens and Functions

Function	Second level Sub-Screen/Description	
VT-d	Supported	
Memory Configuration>	Read only field Memory Configuration: Memory RC Version, Memory Speed, Memory Timings, for Controller #-Channel #-Slot #: Size, Number of Ranks and Manufacturer.	
	Override Performance Downgrade for Mixed Memory	Override to remove performance limitation when mixed memory modules are populated. [Enabled, **Disabled**]
	Memory Test on Warm Boot	Base memory test run in warm boot. [**Enabled,** Disabled]
	Maximum Memory Frequency	Selects maximum memory frequency in MHz. [**Auto**, 1067, 1200, …8400]
	HOB Buffer Size	Selects size of HOB Buffer. [**Auto**, 1B, 1KB, Max(assuming 63 KB total HOB size)]
	Max TOLUD	Maximum value of TOULD. Dynamic adjusts TOULD automatically based on largest MMIO length of installed graphic controller. [**Dynamic**, 1 GB, 1.25 GB,…. 3.5 GB]

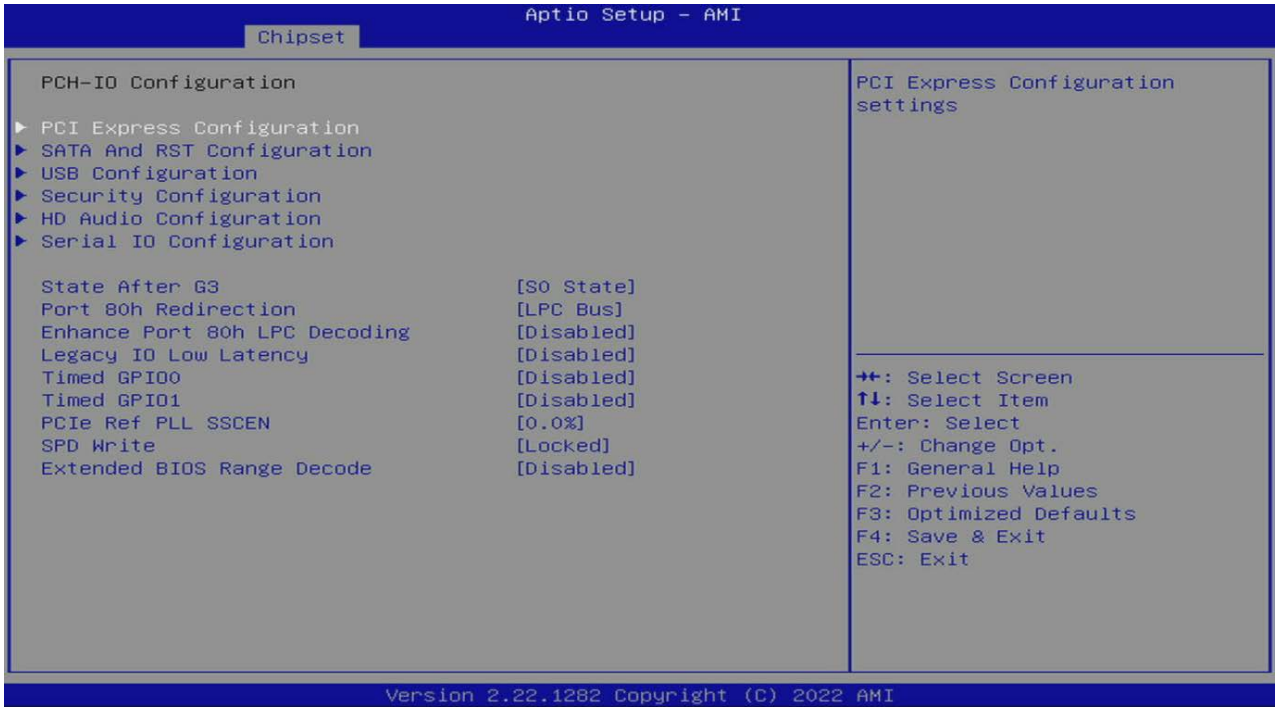
Function	Second level Sub-Screen/Description		
Memory Configuration>	In-Band ECC Support	Enables or disables In-Band ECC. Either IBECC or the TME can be enabled. [Enabled, Disabled]	
	In-Band ECC Error Injection	[Disable]	
	In-Band ECC Operation Mode	[2]	
	Fast Boot	Fast path through the MRC [**Enabled**, Disabled]	
Graphics Configuration>	Skip scanning slots for external Gfx	Enable will not scan for external Gfx cards on PEG and PCH PCIe ports. [Enabled, **Disabled**]	
	Primary Display	Selects which graphics device is the primary display. Hybrid Gfx (HG) can be chosen alternatively. [**Auto**, IGFX, PEG Slot, PCH PCI, Hybrid Gfx]	
	Select PCIE Card	Selects the card used on the platform. [**Auto**, Elk Creek 4, PEG Eval]	
	External Gfx Card Primary Display Configuration>	(Depends on configuration)	
	Internal Graphics	Keep IGfx based on the setup option [**Auto**, Disabled, Enabled]	
	GTT Size	Selects the GTT Size. [2 MB, 4 MB, **8 MB**]	
	Aperture Size	Selects the Aperture Size Note: above 4GB MMIO BIOS assignment is automatically enabled when selecting 2048 MB aperture. To use this feature disable CSM Support. [128 MB, **256 MB**, 512 MB, 1024 MB]	
	DVMT Pre-Allocated	Select DVMT 5.0 pre-allocated (fixed) Graphics Memory size used by the Internal Graphics device. [0 M, 32 M, …**60 M**]	
	DVMT Total Gfx Mem	Select DVMT 5.0 Total Graphics Memory size used by the Internal Graphics device. [128 M, **256 M**, MAX]	
	IGD Configuration>	Read only field IGD Managed by, Intel® GOP Driver, LVDS EEPROM Data, Data Format, Resolution, Color Depth, Channel Count	
		IGD Boot Type	[**Auto**, LFP, LFP2, DP0, DP1, DP2, DP3]
		LFD Panel Type	[**LVDS**, eDP]
		Panel Color Depth	[**18 bit**, 24 bit VESA, 24 bit oLDI]
		Panel Channel Mode	[**Auto**, Single, Dual]
		Backlight Control	[None/External, **PWM**, PWM Inverted, I2C, I2C Inverted]

Function	Second level Sub-Screen/Description		
Graphics Configuration>	IGD Configuration>	PWM Frequency	[**200 Hz**, 400 Hz, 1 kHz, 2, kHz, 4kHz, 8 kHz, 20 kHz, 40kHz]
		Backlight Value	[128]
		LVDS Clock Center Spreading	[**No Spreading**, 0.5%, 1.0%, 1.5%, 2.0%, 2.5%]
		EFP3 (DP0 Type)	[DP with HDMI/DVI]
		EFP4 (DP1 Type)	[DP with HDMI/DVI]
		EFP5 (DP2 Type)	[DP with HDMI/DVI]
		EFP6 (DP3 Type)	[DisplayPort Only]
PEG Port Feature Configuration>	Detect Non-Compliance Device	Detects non-compliance PCI Express device in PEG [Enabled, **Disabled**]	
PEG Width Configuration>	PEG Width Configuration	Sets PEG configuration to 1x16, 2x8 or 1x8+2x4 with lane order controlled by COMe H/W signal or forced to normal or reversed. [**1x16 / H/W**, 1x16 / norm, 1x16 / rev, 2x8 / H/W, 2x8 / norm, 2x8 / rev, 1x8+2x4 / H/W, 1x8+2x4 / norm, 1x8+2x4 / rev]	
VMD Configuration>	VMD controller	[Enabled, **Disabled**]	
PCI Express Configuration>	PCIe Gen4 RP1 (PEG60: opt. NVMe >	PCI Express Root Port #	[**Enabled**, Disabled]
		Connection Type	[Built-in, **Slot**]
		ASPM	[L1, **Disabled**]
		L1 Substrates	[Disabled, L1.1, **L1.1 & L1.2**]
		PCIe 4.0 Speed	[**Auto**, Gen 1, Gen 2, Gen 3, Gen 4]
		IOTG Mode	[Enabled, **Disabled**]
		Transmitter Half Swing	[Enabled, **Disabled**]
		Detect Timeout	[0]
		P2P Support	[Enabled, **Disabled**]
	PCIe Gen4 RP2 (PEG10: x16 or x8 >	PCI Express Root Port #	[**Enabled**, Disabled]
		Connection Type	[Built-in, **Slot**]
		ASPM	[L1, **Disabled**]
		L1 Substrates	[Disabled, L1.1, **L1.1 & L1.2**]
		PCIe 4.0 Speed	[**Auto**, Gen 1, Gen 2, Gen 3, Gen 4]
		IOTG Mode	[Enabled, **Disabled**]

Function	Second level Sub-Screen/Description		
PCI Express Configuration>	PCIe Gen4 RP2 (PEG10: x16 or x8 >	Transmitter Half Swing	[Enabled, **Disabled**]
		Detect Timeout	[0]
		P2P Support	[Enabled, **Disabled**]
Stop Grant Configuration	[**Auto,** Manual]		
VT-d	[**Enabled,** Disabled]		
X2APIC Opt Out	[Enabled, **Disabled**]		
DMA Control Guarantee	[**Enabled**, Disabled]		
Thermal Device (B0:D4:F0)	[Enabled, **Disabled**]		
CPU Crashlog (Device 10)	[**Enabled**, Disabled]		
GNA Device (B0:D8:F0)	SystemAgent Gaussian Network Accelerator [**Enabled**, Disabled]		
CRID Support	SystemAgent CRID and TCSS CRID control for Intel SIPP. [Enabled, **Disabled**]		
WRC Feature	SystemAgent WRC (write cache) features on IOP. When enabled supports IO devices allocating onto the ring and into LLC. [Enabled, **Disabled**]		
VCRt mapping to PEG	[Enabled, **Disabled**]		
Above 4GB MMIO BIOS Assignment	Above 4 GB memory mapping IO BIOS assignment. Note: Enabled automatically when aperture size is set to 2048 MB [**Enabled**, Disabled]		

6.4.3.2. Chipset PCH-IO Configuration Setup Menu

Figure 17: Chipset PCH-IO Configuration Setup menu Initial Screen



The following table shows the Chipset PCH-IO Configuration sub-screens and describes the functions. Default settings are in **bold**.

Table 46: Chipset> PCH-IO Configuration> Menu Sub-screens and Functions

Function	Second level Sub-Screen/Description		
PCI Express Configuration>	COMe PCIe mapping scheme	8x1 (standard)	
	Port8xh Decode	[Enabled, **Disabled**]	
	PCIe Root Port> 1,2,3,4,10,11, 21, 22, 23, 24> (Not mapped to COMe line) PCI Root Port 5 (COM Lane 0)> PCI Root Port 6 (COM Lane 1)> PCI Root Port 7 (COM Lane 2)> PCI Root Port 8 (COM Lane 3)> PCI Root Port 17 (COM Lane 4)> PCI Root Port 18 (COM Lane 5)> PCI Root Port 19 (COM Lane 6)> PCI Root Port 20 (COM Lane 7)> PCI Root Port 9 (opt. device)> PCI Root Port 12 (on-module Ethernet)> PCIe Root Port 13, 14, 15, 16> (Configured as USB/SATA)	PCI Express. Root Port #	Control the PCIe 4.0 Root port. [**Enabled**, Disabled]
		Connection Type	Selects the connection type to root port. [Built-in, **Slot**]
		ASPM	Set ASPM level [**Disabled**, L0s, L1, L0sL1, Auto]
		PME SCI	[**Enabled**, Disabled]
		Hotplug	[Enabled, **Disabled**]
		PCIe Speed	Configure PCIe Speed [**Auto**, Gen 1, Gen 2, Gen 3]
		Detect Timeout	Value in msec the reference code waits for link to exit Detect State for enabled port before assuming there is no

Function	Second level Sub-Screen/Description		
PCI Express Configuration>	PCIe Root Port> 1,2,3,4,10,11, 21, 22, 23, 24> (Not mapped to COMe line) PCI Root Port 5 (COM Lane 0)> PCI Root Port 6 (COM Lane 1)> PCI Root Port 7 (COM Lane 2)> PCI Root Port 8 (COM Lane 3)> PCI Root Port 17 (COM Lane 4)> PCI Root Port 18 (COM Lane 5)> PCI Root Port 19 (COM Lane 6)> PCI Root Port 20 (COM Lane 7)> PCI Root Port 9 (opt. device)> PCI Root Port 12 (on-module Ethernet)> PCIe Root Port 13, 14, 15, 16> (Configured as USB/SATA)	Detect Timeout	device and potentially disabling the port. [0]
		Extra Bus Reserved	Extra Bus reserved for bridges behind this Root Bridge. Range (0-7). [0]
		Reserved Memory	Reserved memory for this Root bridge. Range (1 -20 MB) [10]
		Reserved I/O	Reserved I/O for this root bridge. Range (4K/8K/12K/16K/20K) [4]
SATA and RST Configuration>	SATA Controller	[**Enabled**, Disabled]	
	SATA Mode Selection	[**AHCI**]	
	SATA Speed Limit	[**Auto**, 1.5 Gb/s, 3.0 Gb/s, 6 Gb/s]	
	Software Feature Mask Configuration>	HDD Unlock	Enable indicates the HDD password unlock in the OS is enabled. [**Enabled**, Disabled]
		LED Locate	Enable indicates that LED/SGPIO hardware is attached and Ping to local feature is enabled on OS. [**Enabled**, Disabled]
	SATA Port 0 (PCH SATA0)> SATA Port 1 (PCH SATA1)> Serial ATA Port 2> Serial ATA Port 3>	Port #	SATA Port (0,1,2,3) enabled or disabled. [**Enabled**, Disabled]
		External	Marks port as external. [Enabled, **Disabled**]
		Spin Up Device	Staggered Spin Up performed and only on drives with this option enabled spin up at boot. Otherwise all drives spin up at boot. [Enabled, **Disabled**]
		SATA Device Type	Identifies connected device. [**Hard Disk Drive**, Solid State Drive]
USB Configuration>	xDCI Support	Enables or disables xDCI (USB OTG device) [Enabled, **Disabled**]	
	USB2 PHY Sus Well Power Gating	Enable SUS Well PG for USB2 PHY. This option has no effect on PCH-H. [**Enabled**, Disabled]	

Function	Second level Sub-Screen/Description	
USB Configuration>	USB PD0 Programming	Select enabled if Port Disable Override used. [**Enabled**, Disabled]
	XHCI LTR Mode	[**Enabled**, Disabled]
	USB Overcurrent	Select disabled for pin-based debug. Note: If Pin-based debug is enable but USB over current is not disabled, USB Dbc does not work. [**Enabled**, Disabled]
	USB Overcurrent Lock	Select enabled if over current functionality is used. This makes the xHCI controller consume the overcurrent mapping data. [**Enabled**, Disabled]
	USB Port Disable Override	Enables or disables the USB port from reporting a device connection to the controller. [Enabled, **Disabled**]
Security Configuration>	RTC Memory Lock	Enable locks bytes (38h to 3Fh) in the lower/upper 128 bytes bank of RTC RAM. [**Enabled**, Disabled]
	BIOS Lock	PCH BIOS Lock enable. Note: Enable required for SMM protection of Flash. [**Enabled**, Disabled]
	Force unlock on all GPIO pads	Select enabled to forces all GPIO pads to be in unlocked state. Enabled, **Disabled**]
HD Audio Configuration>	HD Audio>	Controls detection of the HD-Audio device and unconditionally enables or disables the device. [**Enabled**, Disabled]
	Audio DSP	[**Enabled**, Disabled]
	Audio DSP Compliance Mode	Specifies DSP enable system compliance. Note: NHLT (DMIC/BT/I2S configuration) is published for non-UAA only. [non-UAA(IntelSST), **UAA(HAD Inbox/IntelSST)**]
	HD Audio Bus Controller Subsystem ID	Select HD Audio Bus Controller Subsystem ID. [72708086, **300010EC**……..302E10EC]
Serial IO Configuration>	SPI0 Controller & SPI1 Controller	Enables or disables the Serial IO controller. If the given device is function 0 PSF disabling is skipped. PSF default remains and device PCI CFG space is visible. This is needed to allow PCI enumerator access functions above 0 in a multifunction device. The following device depend on each other : I2C 0 & I2C 1,2,3 UART 0 & UART 1, SPI 0,1 UART 2 & I2C 4,5. Note:

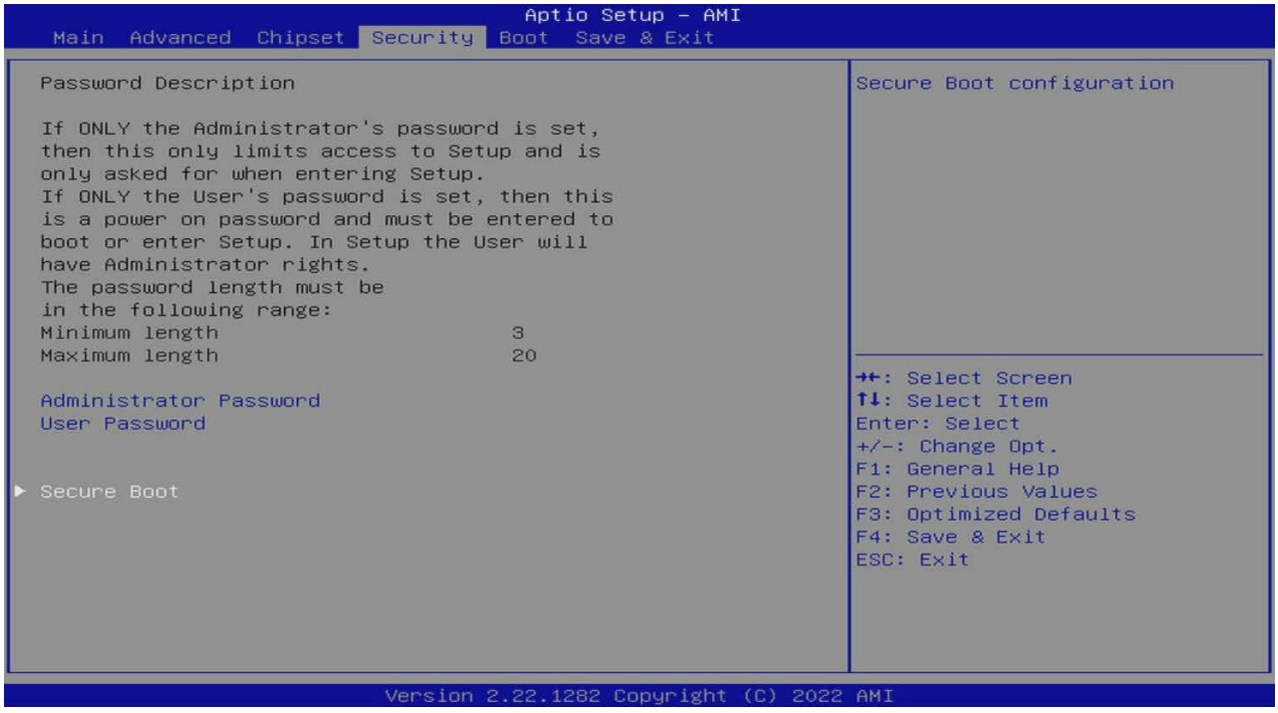
Function	Second level Sub-Screen/Description		
Serial IO Configuration>	SPI0 Controller & SPI1 Controller	UART0 (00:30:00) cannot be disabled when child device is enabled like CNVi Bluetooth (_SB.PC00.UA00.BTH=) UART0 (00:30:00) cannot be enabled when I2S Audio codec is enabled (\SB.PC00.I2C0.HDAC) [Enabled, **Disabled**]	
	UART0 Controller	[Enabled]	
	UART1 Controller	[Enabled]	
	UART2 Controller	[Disabled]	
	Serial IO SPI1 Settings>	ChipSelect 0 polarity	Sets initial polarity of ChipSelect signal. Initial low is with initial idle polarity of low. [Active Low, **Active High**]
		ChipSelect 1 polarity	
	Serial IO UART0 Settings>	Hardware Flow Control	[Disabled]
		Timing parameters disabled	
	Serial IO UART1 Settings>	Hardware Flow Control	[Disabled]
		Timing parameters disabled	
State After G3	Specifies the state to go to when power is reapplied after a power failure (G3 state). [**S0 State**, S5 State]		
Port 80h Redirection	Controls where the port 80h cycles are sent. [**LPC Bus**, PCIE Bus]		
Enhance Port 80h LPC Decoding	Supports the word/dword decoding of port 80h behind LPC. [Enabled, **Disabled**]		
Legacy IO Low Latency	Sets low latency of legacy IO. Note: Some system requires lower IO latency irrespective of power. This is a tradeoff between power and IO latency. [Enabled, **Disabled**]		
Timed GPIO0	Enables or disables Timed GPIO0 Note: disabled will disable cross time stamp time-synchronization as extension of Hammock Harbor time synchronization. [Enabled, **Disabled**]		
Timed GPIO1	Enables or disables Timed GPIO1 Note: disabled will disable cross time stamp time-synchronization as extension of Hammock Harbor time synchronization. [Enabled, **Disabled**]		
PCIe Ref PLL SSCEN	PCIe Ref PLL SC percentage, where Auto keeps hardware default [Auto, **0.0%**, 0.1%, 0.2%, 0.3%, 0.4%, 0.5%]		
SPD Write	Lock or release SPD write capability. For security recommendations, SPD write lock must be set. [**Locked**, Released]		

Function	Second level Sub-Screen/Description
Extended BIOS Range Decoder	Enable causes memory cycles falling in a specific area to be redirected to a SPI flash controller. [Enabled, **Disabled**]

6.4.4. Security Setup Menu

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

Figure 18: Security Setup Menu Initial Screen



The following table shows the Security sub-screen and describes the function. Default settings are in **bold**.

Table 47: Security Setup Menu Sub-screens and Functions

Function	Description	
Administrator Password	Sets administrator password	
User Password	Sets user password	
Secure Boot>	When enabled Platform key (PK) is enrolled and the system is in user mode. The mode change requires platform reset. [Enabled, **Disabled**]	
	Secure Boot Mode	In Custom mode, Secure Boot Policy variables can be configured by a physically present user without full authentication. [**Custom**, Standard]
	Restore Factory Keys	Force system to user mode. Install factory default secure Boot key databases. [Yes, No]
	Reset to Setup Mode	
	Key Management>	Factory Key Provision [Enabled, **Disabled**]
		Restore Factor Keys [Yes, No]

Function	Description	
Secure Boot>	Key Management>	Enroll Efi Image [OK]
		Restore DB Defaults [Yes, No]
	Secure Boot variables (with Size/Keys/Key source)	
		Platform Key
		Key Exchange Keys
		Authorized Signatures
		Forbidden Signatures
		Authorized TimeStamps
		OSRecovery Signatures

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

6.4.4.1. Remember the Password

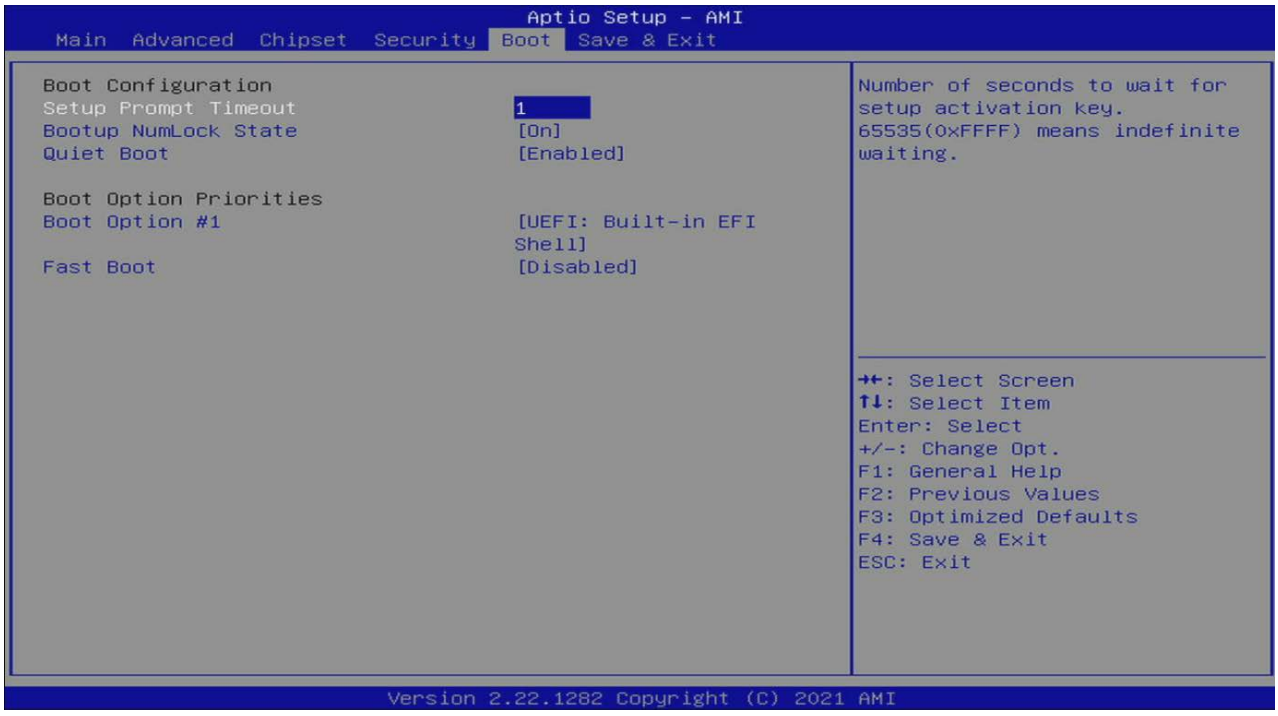
It is highly recommended to keep a record of all passwords in a safe place. Forgotten passwords results in the user being locked out of the system.

If the system cannot be booted because the User Password or the Supervisor Password are not known, clear the UEFI BIOS settings, or contact Kontron Support for further assistance.

6.4.5. Boot Setup Menu

The Boot menu provides functions for booting up the setup program.

Figure 19: Boot Screen Setup Menu Initial screen



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

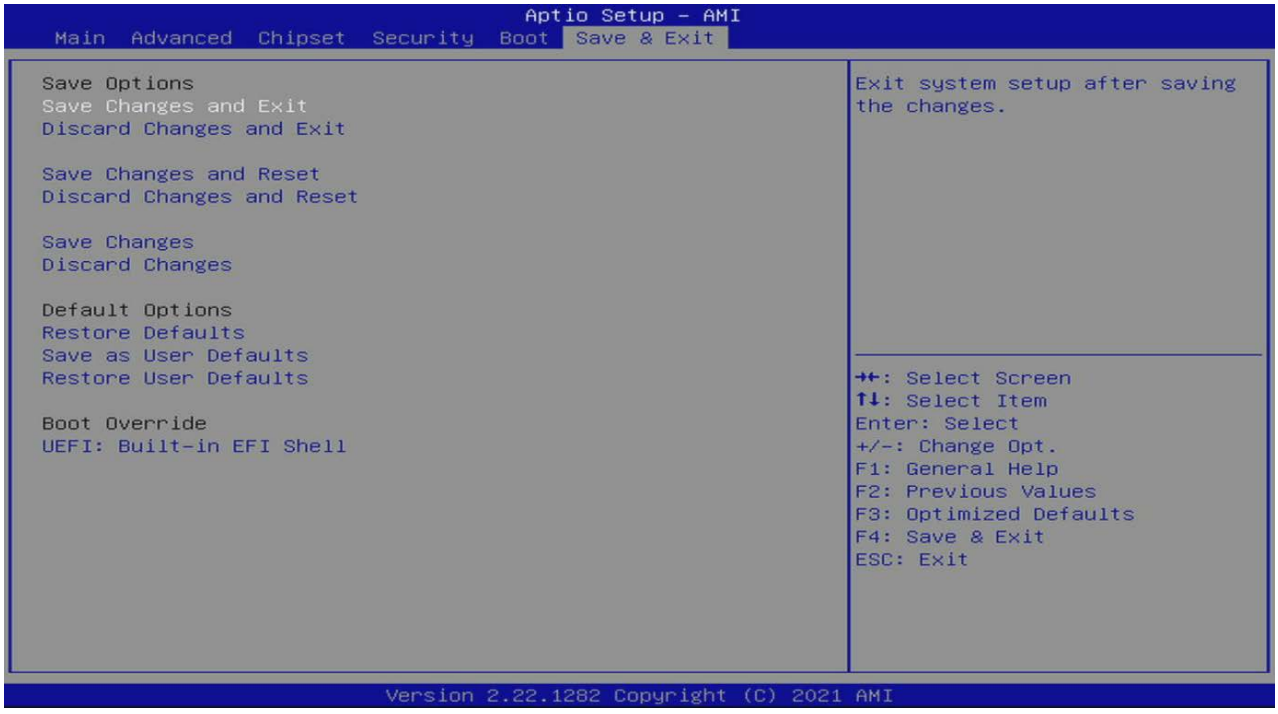
Table 48: Boot Menu Functions

Function	Description
Boot Configuration	
Setup Prompt Timeout	Number of seconds to wait for setup activation key. 65535 (0xFFFF) means indefinite waiting. 1
Bootup NumLock State	[**On**, Off]
Quiet Boot	[**Enabled**, Disabled]
Boot Option Priorities	
Boot Option #1	Set the system boot order [**UEFI: Built-in EFI Shell**, Disabled]
Fast Boot	[Enabled, **Disable**]

6.4.6. Save and Exit Setup Menu

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

Figure 20: Save and Exit Setup Menu Initial Screen



The following table shows the Save and exit sub-screens and describes the function. Default settings are in **bold**.

Table 49: Save and Exit Setup 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
Save as User Defaults	Saves changes made so far as user defaults
Restore User Defaults	Restores user defaults to all setup options
Boot Override	
Boot Override	Attempts to launch the built-in EFI Shell

6.5. 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/.

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

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

6.5.1. Entering the uEFI Shell

To enter the uEFI Shell, follow the steps below:

1. Power on the board.
1. Press the <F7> key (instead of <DEL>) to display a choice of boot devices.
2. Select '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)
```

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

```
Shell>
```

6.5.2. Exiting the uEFI Shell

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

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

6.6. uEFI Shell Scripting

6.6.1. 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. The UEFI shell 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.

6.6.2. 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.

6.6.3. Example of Startup Scripts

6.6.3.1. Execute Shell Script on other Harddrive

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

```
fs0:
bootme.nsh
```

6.7. Firmware Update

Firmware updates are typically delivered as a ZIP archive. Please find the latest available BIOS-ZIP archive on Kontron's Customer Section. Further information about the firmware update procedure can be found in the included "flash_instruction.txt"-file.

Register for Kontron's Customer Section to get access to BIOS downloads and PCN service.

7/ 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.

7.1. 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.

7.2. 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: RMA Information | Kontron Europe and Asia

2. 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.

3. 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

4. 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.

5. 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.

List of Acronyms

Table 50: List of Acronyms

ACPI	Advanced Configuration and Power Interface
API	Application Programming Interface
BIOS	Basic Input Output System
bps	bits per second
BSP	Board Support Package
Carrier Board	Application specific circuit board that accepts a COM Express ® module
COM	Computer-on-Module
COMe-b	COM Express® b=basic 125 mm x 95 mm module form factor
COMe-c	COM Express® c=compact 95 mm x 95 mm module form factor
COMe-m	COM Express® m=mini 84 mm x 55 mm module form factor
CPU	Central Processing Unit
DDC	Display Data Control
DDI	Digital Display Interface –
DDIO	Digital Display Input/Output
DDR	Double Data Rate
DIMM	Dual In-line Memory Module
DP	Display Port
DP	Differential Pair
DMA	Direct Memory Access
DRAM	Dynamic Random Access Memory
DVI	Digital Visual Interface
EAPI	Embedded Application Programming Interface
ECC	Error Checking and Correction
EEPROM	Electrically Erasable Programmable Read-Only Memory
EDID	Extended Display Identification Data
eDP	Embedded Display Port
EMC	Electromagnetic Compatibility (EMC)
ESD	Electro Sensitive Device
FAT	File Allocation Table
FIFO	First In First Out
Gb	Gigabit
GBE	Gigabit Ethernet
GPI	General Purpose Input
GPIO	General Purpose Input Output
GPO	General Purpose Output
HDA	High Definition Audio (HD Audio)
HD/HDD	Hard Disk /Drive
HDMI	High Definition Multimedia Interface
HWM	Hardware Monitor
I²C	Inter integrated Circuit Communications
I/O	Input/Output
IOT	Internet of Things
ISA	Industry Standard Architecture
JILI	JUMPtec Intelligent LVDS Interface
LAN	Local Area Network
LPC	Low Pin-Count Interface:
LPT	Line Printing Terminal
LVDS	Low Voltage Differential Signaling
ME	Management Engine
MLC	Multi Level Cell
MTBF	Mean Time Before Failure
NA	Not Available
NC	Not Connected
OA	Open Analog
OD	Open Drain
OS	Operating System
PCH	Platform Controller Hub
PCI	Peripheral Component Interface
PCIe	PCI-Express
PD	Pull Down
PECI	Platform Environment Control Interface
PEG	PCI Express Graphics
PICMG®	PCI Industrial Computer Manufacturers Group
PHY	Ethernet controller physical layer device
Pin-out Type	COM Express® definitions for signals on COM Express® Module connector pins.
pSLC	pseudo Single Level Cell
PSU	Power Supply Unit
PTT	Platform Trust Technology
PU	Pull Up
PWR	Power
RoHS	Restriction of the use of certain Hazardous Substances
RST	Rapid Storage Technology
RTC	Real Time Clock
SATA	Serial AT Attachment
SFX	Small Formfactor ATX
SGMII	Serial Gigabit Media Independent Interface
SIPP	Stage Image Platform Program
SLC	Single Level Cell
SMB	System Management Bus
SoC	System on a Chip
SOIC	Small Outline Integrated Circuit
SPI	Serial Peripheral Interface
TCC	Time Coordinated Computing
TBD	To Be Decided
TIM	Thermal Interface Material
TPM	Trusted Platform Module
TSN	Time Sensitive Networking
UART	Universal Asynchronous Receiver Transmitter
UEFI	Unified Extensible Firmware Interface
USB	Universal Serial Bus
VGA	Video Graphics Adapter
WDT	Watch Dog Timer
WEEE	Waste Electrical and Electronic Equipment
WOL	Wake On LAN

About Kontron

Kontron is a global leader in IoT/Embedded Computing Technology (ECT). 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 Europe GmbH

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