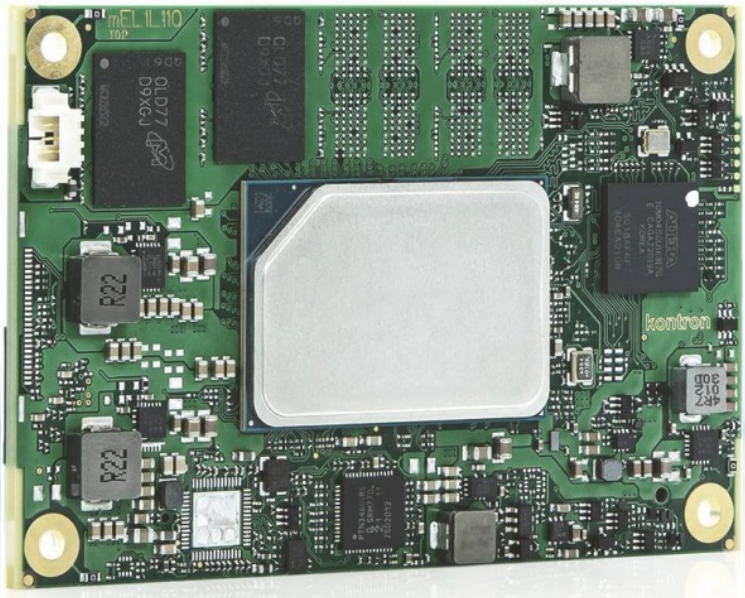
USER GUIDE



COMe-mEL10

User Guide Rev. 1.1

Doc. ID: 1067-7493

This page has been intentionally left blank

COME-MEL10 - USER GUIDE

Disclaimer

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

Kontron Europe GmbH

Gutenbergstraße. 2
85737 Ismaning
Germany
www.kontron.com

Intended Use

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

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

Revision History

Revision	Brief Description of Changes	Date of Issue	Author/ Editor
1.0	Initial version	2021-July-23	CW
1.1	Added Tjuntion temperature range to Table 5: Processor Specification	2021-Sept-09	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: https://www.kontron.com/support-and-services/kontron-europe-and-asia/support/contact-support

Customer Service

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

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

Customer Comments

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

Symbols

The following symbols may be used in this user guide

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

For Your Safety

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

High Voltage Safety Instructions

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

⚠CAUTION

Warning

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

⚠CAUTION

Electric Shock!

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

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

Special Handling and Unpacking Instruction

NOTICE

ESD Sensitive Device!

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

⚠CAUTION

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

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

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

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

Lithium Battery Precautions

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

⚠CAUTION

Danger of explosion if the battery is replaced incorrectly.

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

General Instructions on Usage

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

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

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

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

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

Quality and Environmental Management

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

Disposal and Recycling

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

WEEE Compliance

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

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

Environmental protection is a high priority with Kontron.

Kontron follows the WEEE directive

You are encouraged to return our products for proper disposal.

Table of Contents

List of Tables

List of Figures

1/ Introduction

This user guide describes the COMe-mEL10 module made by Kontron and focuses on describing the modules special features. Kontron recommends users to study this user guide before powering on the module.

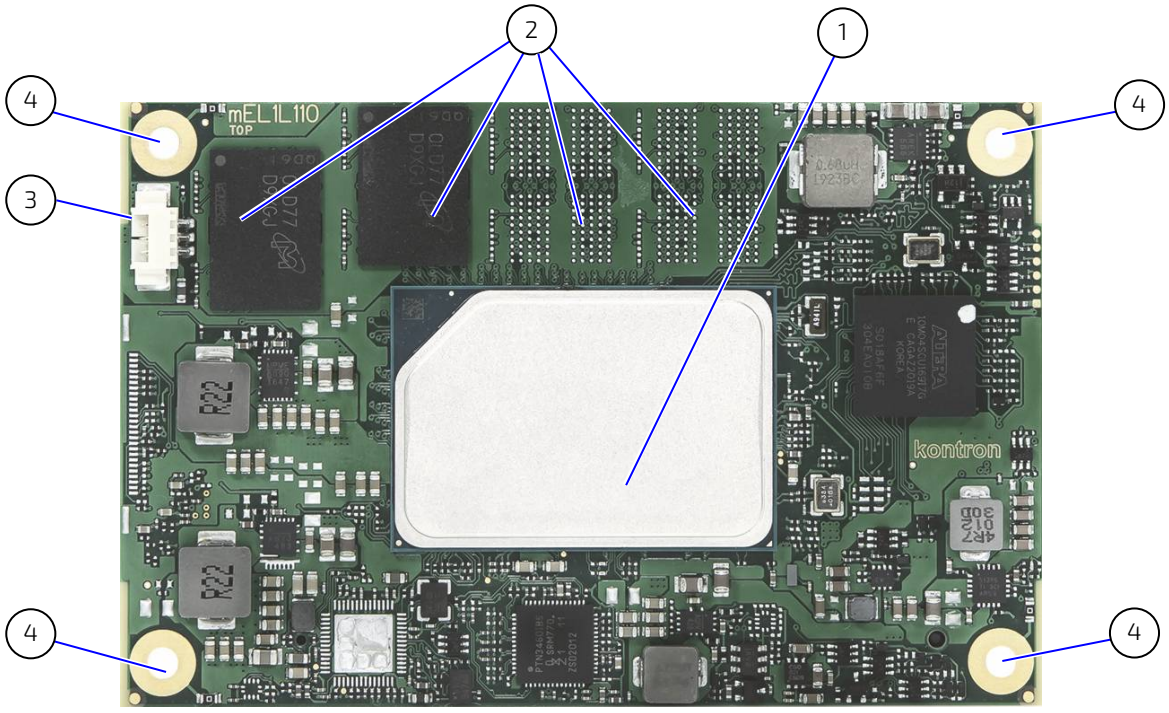
1.1. Product Description

The COMe-mEL10 is small form factor COM Express® type 10 Computer-On-Module designed for flexible implementation within multiple embedded industrial environments. The COMe-mEL10 is based on the Intel® Multi Chip Package (MCP) Atom™, Pentium® and Celeron® processors with an integrated PCH to combine increased efficiency and performance with TDP as low as 6 W and no more than 12 W, and includes Intel's® extensive HD Graphics capabilities.

Key COMe-mEL10 features are:

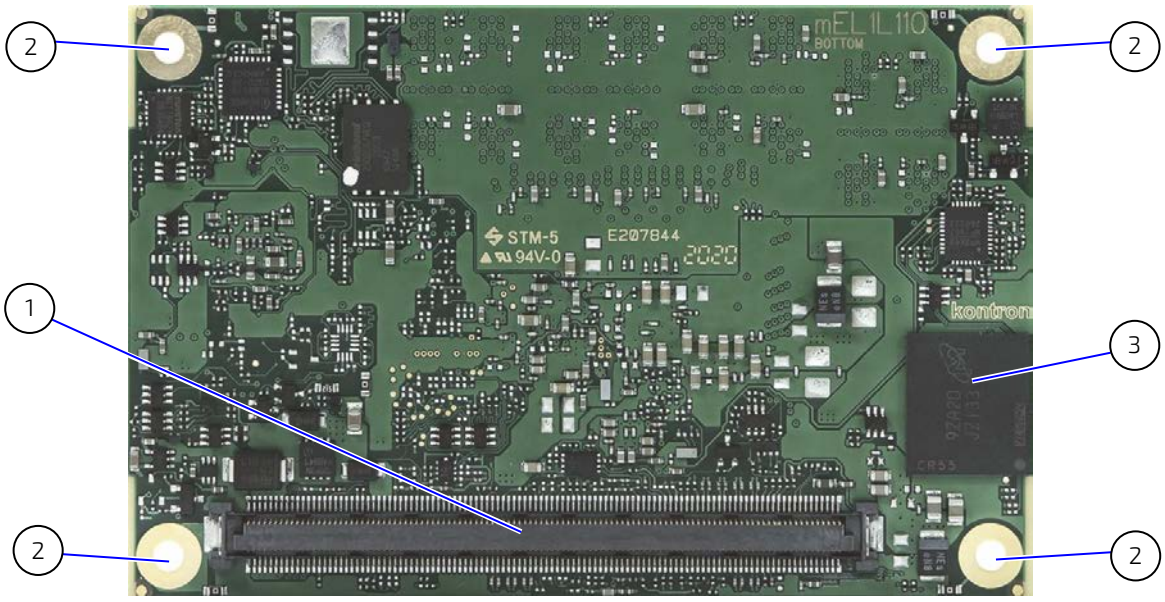
- Intel® Multi Chip Package series of Atom™, Pentium® and Celeron® processors
- Small form-factor COM Express® mini Type 10 pinout, compatible with PICMG COM.0 Rev 3.0 spec
- Up to 16 GByte LPDDR4 memory down (with in-band ECC)
- High-speed connectivity 4x PCI Express, 1x 1 Gb Ethernet, 2x USB 3.1 + 6x USB 2.0, 2x SATA Gen.3
- Support for Industrial and commercial temperature grade environments

Figure 1: COMe-mEL10 Front Side



1	Multi-Chip Package (MCP)	3	3-pin fan connector
2	Up to 4 memory chips depending on the capacity	4	4x mounting points for standoffs

Figure 2: COM-mEL10 Bottom Side



1	COMe interface connector (X1A)	2	4x Mounting points for stand offs
		3	eMMC

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
  - EL
- 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 information about the COM Express® specification, visit the PCI Industrial Computer Manufacturers Group (PICMG®) website.

1.4. COM Express® Functionality

All Kontron COM Express® mini modules contain one 220-pin connector containing two rows called row A & row B. The COM Express® mini Computer-On-Module (COM) features the following maximum amount of interfaces according to the PICMG module pinout type.

Table 1: Type 10 and COMe-mEL10 Functionality

Feature	Type 10	COMe-mEL10
HD Audio	1x	1x
Gbit Ethernet	1x	1x
Serial ATA Gen3	2x	2x
PCI Express x 1	4x	Up to 4x
PCI Express x16 (PEG)		
USB Client	1x	1x (Port 7 is dual role Client/Host)
USB	2x USB 3.0/2.0 6x USB 2.0	2x USB 3.1 Gen 2/USB 2.0 6x USB 2.0
LVDS (eDP)	1x LVDS single 24-bit channel (with eDP overlay)	1x LVDS single 24-bit channel (with eDP overlay)
DP++ (DP/HDMI/DVI)	1x	1x
SPI	1x	1x
LPC /eSPI	1x	1x
External SMB	1x	1x
I2C	1x	1x
GPIO or SDIO	8x	8x GPIO (with SDIO overlay option)
UART (2-wire COM)	2x	2x
TPM 2.0	1x	1x
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 COMe-mEL10 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 commercial and industrial 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)

Product Number	Product Name	Description
34012-0416-N1-2	COMe-mEL10 N6211 4G/16G	COM Express® mini pin-out type 10 with Intel® Celeron® N6211, 2 core, 1.2GHz, 4GB LPDDR4-3200 memory down, GPY115 LAN, 16GB eMMC MLC, commercial temperature
34012-0432-J2-4	COMe-mEL10 J6426 4G/32G	COM Express® mini pin-out type 10 with Intel® Pentium® J6426, 4 core, 2.0GHz, 4GB LPDDR4-3733 memory down, GPY115 LAN, 32GB eMMC MLC, commercial temperature

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

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

Product Number	Product Name	Description
34013-0416-R1-2	COMe-mEL10 E2 x6212RE 4G/16G	COM Express® mini pin-out type 10 with Intel® Atom®x6212RE , 2 core, 1.2GHz, 4GB LPDDR4-3200 memory down, GPY115 LAN, 16GB eMMC MLC, industrial temperature
34013-0432-R1-4	COMe-mEL10 E2 x6414RE 4G/32G	COM Express® mini pin-out type 10 with Intel® Atom® x6414RE, 4 core, 1.5GHz, 4GB LPDDR4-3200 memory down, GPY115 LAN, 32GB eMMC MLC, industrial temperature
34013-0832-R2-4	COMe-mEL10 E2 x6425RE 8G/32G	COM Express® mini pin-out type 10 with Intel® Atom® x6425RE , 4 core, 1.9GHz, 8GB LPDDR4-4267 memory down, GPY115 LAN, 32GB eMMC MLC, industrial temperature

2.2. Accessories

The accessories are module specific, COMe-type 10 specific, or general COMe accessories. For more information, visit the COMe-mEL10 web page or contact your local Kontron Sales Representative or Kontron Inside Sales.

Table 4: Accessories

Part Number	Carrier	Description
34101-0000-00-2	COMe Eval Carrier T10 GEN2	COM Express® Evaluation Carrier Type 10 Gen 2

Part Number	Carrier	Description
34105-0000-00-x	COMe RefCarrier-i T10 TNIP	COM Express® Reference Carrier-i Type 10 Thin-nano ITX Professional

Part Number	Heatspreader	Description
34013-0000-99-0	HSP COMe-mEL10 (E2) THREAD	Heatspreader for COMe-mEL10 commercial and E2, threaded mounting holes
34013-0000-99-1	HSP COMe-mEL10 (E2) THROUGH	Heatspreader for COMe-mEL10 commercial and E2, through holes
34013-0000-99-2	HSP COMe-mEL10 (E2) SLIM THREAD	Heatspreader slimline 6.5mm for COMe-mEL10 commercial and E2, threaded mounting holes
34013-0000-99-3	HSP COMe-mEL10 (E2) SLIM THROUGH	Heatspreader slimline 6.5mm for COMe-mEL10 commercial and E2, through holes

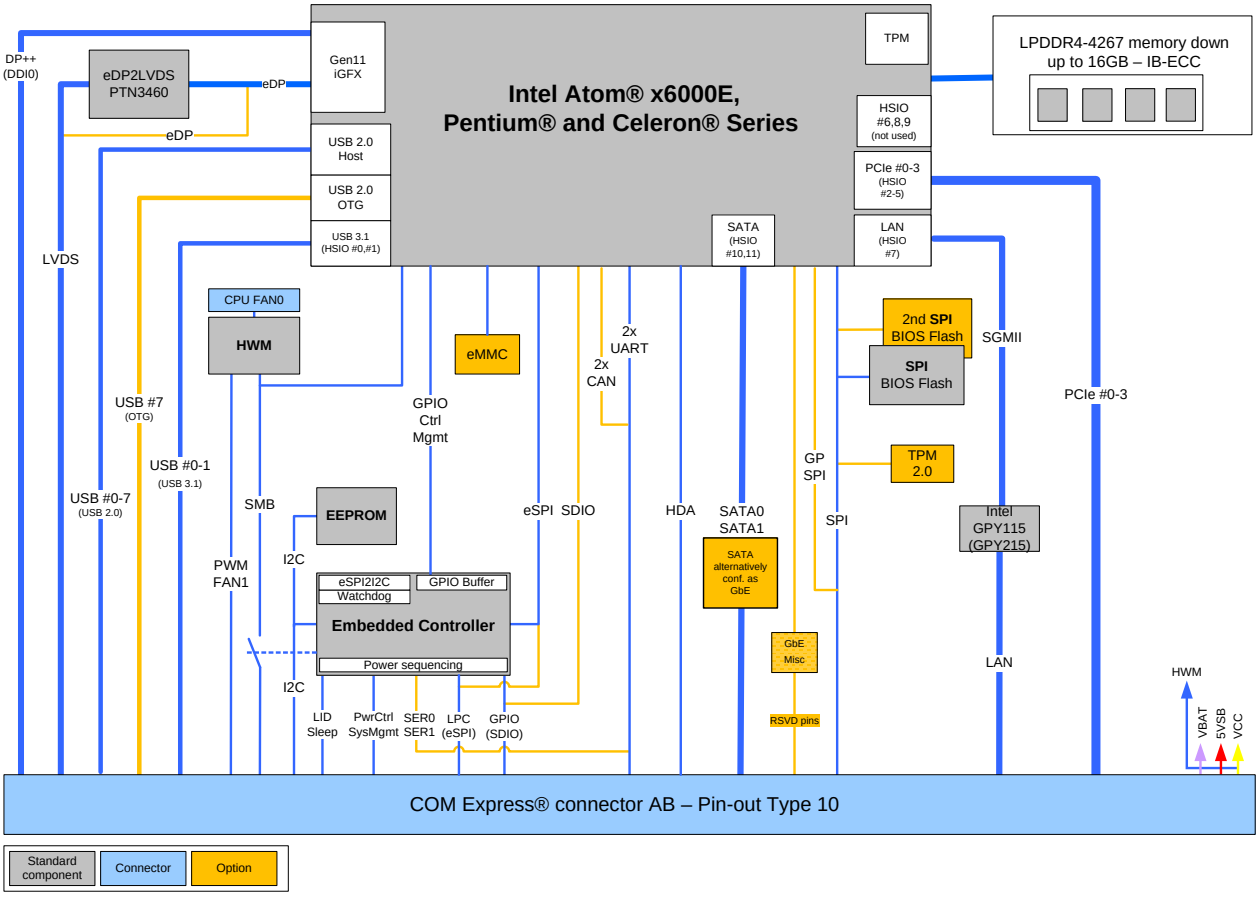
Part Number	Fan Cables	Description
96079-0000-00-0	KAB-HSP 200 mm	Cable adapter to connect fan to module (COMe Basis/Compact/Mini)
96079-0000-00-2	KAB-HSP 40 mm	Cable adapter to connect fan to module (COMe Basis/Compact/Mini)

Part Number	Cooling Solution	Description
34099-0000-99-0	COMe mini Active Uni Cooler (w/o HSP)	Active universal cooler without heatspreader
34099-0000-99-1	COMe mini Passive Uni Cooler (w/o HSP)	Passive universal cooler without heatspreader
34099-0000-99-3	COMe mini Passive Uni Cooler top mount	Passive universal cooler top mountable

2.3. Functional Specification

2.3.1. Block Diagram

Figure 3: Block Diagram COMe-mEL10



2.3.2. Processors

The COMe-mEL10 is based on the Intel® series of Multi Chip Package (MCP) Atom™ X6000E series, Pentium® and Celeron® processors, with a Platform Controller Hub (PCH) on the same package (compact Type 3 BGA 35 mm x 24 mm package).

The processor variants support the following technologies:

- Intel® 64 Architecture
- Intel® Gen 11 GFX graphics
- Intel® Programmable Service Engine (PSE)
- Intel® Virtualization Technology (VT-2) with extended pages and (VT-d) for directed I/O
- Real time computing with Time Coordinated Computing (TCC)
- Thermal Management with Intel® Thermal Monitor (TM1 and TM2)
- Power Management with Intel® Speedstep® Technology
- Security with Intel® Boot Guard device protection, Secure Key and Intel® AES NI

The following table lists the specification of the COMe-mEL10 processor variants.

Table 5: Processor Specification

Intel®		Celeron®	Pentium®	Celeron®	Pentium®
		J6413	J6426	N6211	N6415
# of Cores		4	4	2	4
# of Threads		4	4	2	4
Cache		1.5 MByte	1.5 MByte	1.5 MByte	1.5 MByte
Base Frequency		1.8 GHz	2.0 GHz	1.2 GHz	1.2 GHz
Turbo Frequency (Max.)		3.0 GHz	3.0 GHz	3.0 GHz	3.0 GHz
Graphic Gen 11 GFX		16 EU	32 EU	16 EU	16 EU
Thermal Design Power (TDP)		10 W	10 W	6.5 W	6.5 W
Memory Types/Speed		LPDDR4-3733	LPDDR4-3733	LPDDR4-3200	LPDDR4-3200
Memory Channels (Max.)		4	4	4	4
Memory Size (Max.)		16 GB	16 GB	16 GB	16 GB
ECC Memory		No	No	No	No
PCIe Express Configurations		4 x1 1 x2 + 2 x1 2 x2 1 x4	4 x1 1 x2 + 2 x1 2 x2 1 x4	4 x1 1 x2 + 2 x1 2 x2 1 x4	4 x1 1 x2+ 2 x1 2 x2 1 x4
Max. # PCIe Lanes		4	4	4	4
Premium IO		Intel®PSE	Intel®PSE	Intel®PSE	Intel®PSE
Use Condition		PC Client	PC Client	PC Client	PC Client
Tjunction	Min.	0°C	0°C	0°C	0°C
	Max.	+105°C[2]	+105°C[2]	+105°C[2]	+105°C[2]

Intel®	Atom™	Atom®	Atom®	Atom™	Atom™	Atom™
	X6211E	X6413E	X6425E	X6212RE	X6414RE	X6425RE
# of Cores	2	4	4	2	4	4
# of Threads	2	4	4	2	4	4
Cache	1.5 MByte	1.5 MByte	1.5 MByte	1.5 MByte	1.5 MByte	1.5 MByte
Base Frequency	1.3 GHz	1.5 GHz	2.2 GHz	1.2 GHz	1.5 GHz	1.9 GHz
Turbo Frequency (Max.)	3.0 GHz	3.0 GHz	3.0 GHz	NA	NA	NA
Graphic Gen 11 GFX	16 EU	16 EU	32 EU	16 EU	16 EU	32 EU
Thermal Design Power (TDP)	6 W	9 W	12 W	6 W	9 W	12 W
Memory Types/Speed	LPDDR4-3200	LPDDR4-3200	LPDDR4-3733	LPDDR4-3200	LPDDR4-3200	LPDDR4-4267
Memory Channels (Max.)	4	4	4	4	4	4
Memory Size (Max.)	16 GB	16 GB	16 GB	16 GB	16 GB	16 GB
ECC Memory	In band	In band	In band	In band	In band	In band
PCIe Express Configurations	4 x1 1 x2 + 2 x1 2 x2 1 x4	4 x1 2 x1 + 1 x2 2 x2 1 x4	4 x1 2 x1 + 1 x2 2 x2 1 x4	4 x1	4 x1 2 x1 + 1 x2 2 x2 1 x4	4 x1 2 x1 + 1 x2 2 x2 1 x4
Max. # PCIe Lanes	4	4	4	4	4	4

Intel®		Atom™	Atom®	Atom®	Atom™	Atom™	Atom™
		X6211E	X6413E	X6425E	X6212RE	X6414RE	X6425RE
Premium IO		Intel®PSE	Intel®PSE	Intel®PSE	Intel®PSE/TSN Intel®TCC	Intel®PSE/TSN Intel®TCC	Intel®PSE/TSN Intel®TCC
Use Condition		Embedded	Embedded	Embedded	Industrial[1]	Industrial[1]	Industrial[1]
Tjunction	Min.	-40°C	-40°C	-40°C	-40°C	-40°C	-40°C
	Max.	+105°C[2]	+105°C[2]	+105°C[2]	+110°C[2]	+110°C[2]	+110°C[2]

[1] Recommendation for 24/7 applications.

[2] **PC Client CPU**: with Tjunction limits the max. temperature range during operation is +-70°C starting from boot time temperature

Embedded / Industrial CPU: within Tjunction limits the max. temperature range during operation is +-90°C starting from boot time temperature

The behavior is described in Intel document #636112 as DTR = Dynamic Temperature Range. For more information or a higher DTR-value, contact Kontron Support.

The features specified in Table 5: Processor Specification may not be compatible with the COMe-mEL10 features. For specific COMe-mEL10 features, see the relevant section in Chapter 2.3:Funtional Specification.

2.3.3. Platform Controller Hub (PCH)

The COMe-mEL10's Multi Chip Package (MCP) includes an integrated Platform Controller Hub (PCH).

2.3.4. System Memory

The COMe-mEL10 supports LPDDR4-4267 memory down with up to four channels supporting 32 Gbit, for a maximum total capacity of 16 GByte for both industrial and commercial temperature graded variants.

The following table lists specific system memory down features.

Type	LPDDR4-4267 / LPDDR4-3200
Memory Densities	16 Gbit, 32 Gbit
Memory Channels	4
Memory Capacity (Max.)	16 GByte
Maximum Speed	4267 MT/s for single rank memory only (system capacity <=8 GByte) 3200 MT/s for dual rank memory only (system capacity >8 GByte)
ECC [1]	In band ECC

[1] In-band ECC improves safety and reliability by providing ECC protection to specific regions of the physical memory. Out of band ECC is not supported.

For memory capacities higher than 8 GByte the maximum speed is limited to 3200 MT/s. The maximum speed of 4267 MT/s is only available for single rank memory. Dual rank memory is limited to 3200 MT/s. However, it must be noted that maximum memory speed depends on CPU capability.

2.3.5. Graphics (LVDS or eDP, and DP++)

The COMe-mEL10 supports up to two simultaneous displays on the Digital Display Interface (DDI), where DDI0 (port A) is LVDS by default with the option to overlay to eDP requiring a hardware assembly and DDI1 (port B) supports DP++.

The following table lists the display features.

DDI	Display Interface	Description	Max. Resolution
DDI0 (port A)	LVDS (default)	Single channel 24-bit color (1 pixel per clock)	1920 x 1200 @ 60Hz
	eDP (option)	eDP overlay option requires hardware assembly	4096 x 2160 @ 60Hz
DDI1 (port B)	DP 1.2 V (DP++)	4K resolution with multiple active displays	4096 x 2160 @ 60Hz

Supported Flat panels with Extended Display identification Data (EDID)/DisplayID.

It is recommended to only use a DP-to-HDMI or DP-to-DVI passive adapter compliant to the VESA DP Dual-Mode standard. Display detection issues may occur with use of with FET level shifter adapters for DDC translation.

At 4K resolution, to increase link margin a DP redriver on the carrier is recommended.

2.3.6. HD Audio

The COMe-mEL10 supports HD audio for up to two external codecs.

Type	Intel® HD Audio
# Audio devices	2x external codec

The HD Audio codec frequency is selected in the BIOS setup: PCH-IO Configuration> HD Audio Configuration> HD Audio Advanced Configuration> HD Audio Link Frequency> [6 MHz, 12 MHz, 24 MHZ].

2.3.7. PCI Express Lanes [0-3]

The COMe-mEL10 supports up to four high-speed PCI Express 3.0 lanes PCIe [0-3], allowing for the connection of up to four separate external PCIe devices. The default PCIe configuration is (4 x1) with options for (2 x1 + 1 x2), (2 x2) and (1 x4).

The following table lists the supported PCI Express lane configurations.

COMe Connector	HSIO lane	HSIO Port	Supported Lane Configuration			
			4 x1 (default)	2 x1 + 1 x2	2 x2	1 x4
PCIE_0	2	PCIe #0	x1	x2	x2	x4
PCIE_1	3	PCIe #1	x1			
PCIE_2	4	PCIe #2	x1	x1	x2	
PCIE_3	5	PCIe #3	x1	x1		

To change the default PCIe configuration (4x1), a new BIOS version is required. For BIOS version information, visit Kontron's Customer Section or contact Kontron Support.

2.3.8. USB

The COMe-mEL10 supports two USB 3.1 Gen2 ports backwards compatible with USB 2.0 and six dedicated USB 2.0 ports. The USB Client is an option and if implemented one USB 2.0 port is required to support the USB client functionality. The USB client can be implemented on any USB 2.0 port supporting dual role capabilities. Dynamic changing is not possible. Select the USB 2.0 client port in the BIOS set up and reset the BIOS.

The following table lists the supported USB features.

USB Ports	2x USB 3.1 Gen2 (10 Gb/s) (USB 2.0 backwards compatible) 6x USB 2.0
USB Over Current Signals	4x
USB Client Port	1 x USB 2.0 host/client mode (option)

The following table lists the USB 3.1 port connections.

COMe Connector	HSIO Lane	HSIO Port	Description
USB_SS1	0	USB#0	USB 3.1 Gen 2 (10 Gb/s) dual role port
USB_SS2	1	USB#1	USB 3.1 Gen 2 (10 Gb/s) dual role port

The USB speed can be changed in the BIOS setup menu: Chipset> PCH/IO Configuration> USB Configuration> USB3 Link Speed> GEN1, GEN2.

When designing the carrier board consider the speed of the USB 3.1 Gen 2 (10 Gb/s). Kontron recommends using a retimer/redriver on the carrier.

The following table lists the USB 2.0 port connections.

COMe Connector	PCH USB Port	Description
USB0	USB2_0	USB 2.0 port
USB1	USB2_1	USB 2.0 port
USB2	USB2_2	USB 2.0 port
USB3	USB2_3	USB 2.0 port
USB4	USB2_4	USB 2.0 port
USB5	USB2_5	USB 2.0 port
USB6	USB2_6	USB 2.0 port
USB7	USB2_7	USB 2.0 port dual role USB Host

2.3.9. SATA

The COMe-mEL10 supports two SATA high-speed storage interface (6 Gb/s) lanes.

The following table lists the SATA connector connections.

COMe Connector	HSIO lane #	HSIO Port	Description
SATA0	10	SATA#0	SATA Gen 3, 6 Gb/s
SATA1	11	SATA #1	SATA Gen 3, 6 Gb/s

2.3.10. Ethernet LAN

The COMe-mEL10 supports one Ethernet port with speeds of 1 Gb/s or on request up to 2.5 Gb/s.

The main Ethernet PHY features are:

- Full and half duplex 10Base-T(e), 100Base-T, 1000Base-T and on request 2.5 GBase-T
- Precise time stamping according to IEEE 1588 V2 and Synchronous Ethernet (SyncE)
- Smart AZ for legacy MAC to support IEEE 802.3az power saving in idle mode
- Auto MDI/MDI-X and auto polarity correction
- Wake on LAN (WOL)
- Jumbo frame up to 10 KB
- Auto down for Cat3 (four wire) or bad cable

The following table lists the Ethernet external PHY port connections

COMe Connector	HSIO lane #	HSIO Port	Description
GBE0_MDI[0:3]	7	GBE#0	10/100/1000 Base-T or 2.5 GBase-T

For 2.5 Gb/s Ethernet port speed, Intel® recommends the use of a compatible connector.

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

2.3.11. COMe High-speed Serial Interfaces Overview

The COMe-mEL10 supports 12 high-speed serial input output lanes for PCIe Gen 3.0, USB 3.1, SATA, GBE and Universal Flash Storage (UFS).

The following table lists the high-speed lane combinations.

HSIO Lane	High-Speed IO				Description
	USB 3.1	PCIE Gen 3.0	GbE	SATA 3.0	
0	USB#0				USB 3.1 Super Speed Gen 2 (10 Gb/s)
1	USB#1				USB 3.1 Super Speed Gen 2 (10 Gb/s)
2		PCIe#0			PCIe 3.0 lane
3		PCIe#1			PCIe 3.0 lane
4		PCIe#2			PCIe 3.0 lane
5		PCIe#3			PCIe 3.0 lane
6					Not connected
7			GbE#0		GbE (1 Gb/s or optional 2.5 Gb/s)
8					Not connected
9					Not connected
10				SATA#0	SATA Gen 3, 6 Gb/s
11				SATA#1	SATA Gen 3, 6 Gb/s

2.3.12. Storage

The COMe-mEL10 support the following storage features.

eMMC	1x eMMC 5.1 NAND Flash (option) Capacity: up to 64 GB pSLC or up to 128 GB MLC
Embedded EEPROM (EeeP)	1x Eeep (EEprom available on address A0h 8-bit/50h 7-bit)

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

2.3.13. BIOS/Software Features

The following table lists the supported BIOS and software features.

BIOS EFI	AMI Aptio V uEFI
Software	Demo Utility for KEAPI 3.0 usage for all supported OS BIOS/ EFI Flash Utility for EFI shell, Windows 10 and Linux BIOS/EFI Utility to configure PCIe mapping BIOS/EFI Utility for users to implement Boot Logo and customized NVRA
Operating System (OS)	Board Support Packages for: ▶ Windows 10 (IOT) Enterprise x64 ▶ Yocto Linux (64 bit) incl. PLD driver and Live-CD ▶ VxWorks 7.x, x64
Custom BIOS Settings/ Flash Backup	Supported

2.3.14. Features

The following table lists General, Special and Optional COMe-mEL10 features.

General Features	
SPI	On-module and external carrier boot from SPI
LPC	LPC bus (default) pins shared with eSPI (eSPI overlay on request)
LID Signal	Supported
Sleep Signal	Supported
SM Bus	supported
Fast I2C	Connected to module EEPROM, carrier EEPROM and RTC clock
Watchdog Support	Dual staged
RTC	Internal RTC (with external RTC on request)
Display (DDI)	Up to 4k resolutions

Special Kontron Features	
Temperature Grade	Industrial grade temperature
Embedded API	KEAPI 3.0 (included in reference image)

Optional Features	
eMMC Flash	Up to 64 GByte pSLC and up to 128 GByte MLC
eDP instead of LVDS	LVDS signals can be overlaid with eDP signals
eSPI instead of LPC	eSPI instead of LPC on the COM connector
UART	2x RX/TX
USB Client	1x USB Client
TPM 2.0	Dedicated TPM chip

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 COMe-mEL10 supports a supply voltage of 12 V (single power rail voltage) and a wide input voltage range of 4.75 V to 20 V. Other supported voltages are 5 V standby and 3.3 V RTC battery input.

Table 6: COMe-mEL10 Electrical Specification

Supply Voltage (VCC) (range)	4.75 V to 20 V
Supply Voltage (VCC) (nominal)	12 V
Standby Voltage	5 V ±5 % Note: 5V Standby voltage is not mandatory for operation
RTC Voltage	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 100 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 COMe-mEL10 implements the Advanced Configuration and Power Interface (ACPI) 6.0 hardware specification with 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 state (S5)

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

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 7: 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 an external battery manager is present and SMB_ALERT # connected, the module always powers on even if the BIOS switch "After Power Fail" is set to "Stay Off".
Battery low (BATLOW#)	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 COMe-mEL10 supports single power supply mode and ATX power supply mode. To change the power supply mode set the ATX mode and single power supply mode setting as described in the following chapters.

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 ramps up the PCH enters the 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 the 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 4.75V.

The input voltage must always be higher than 5 V standby (VCC>5VSB) for modules supporting a wide input voltage range down to 4.75 V.

Table 8: 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 4.75 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 9: 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 and Metal Heat Slug

A heatspreader plate (HSP) assembly is NOT a heat sink. The heatspreader plate works as a COM Express® standard thermal interface to be used in conjunction with a heat sink or external cooling devices. External cooling must be provided to maintain the heatspreader plate at proper operating temperatures. Under worst-case conditions, the cooling mechanism must maintain an ambient air and heatspreader plate temperature on any spot of the heatspreader's surface according to the module specifications:

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

Commercial temperature grade variants have no preconfigured Intel® heatspreader and the supplied metal heat slug (packed separately in the delivery box for the heatspreader) must be installed.

Industrial temperature grade variants have a preconfigured Intel® heatspreader and do not require the metal heat slug to be installed.

For industrial temperature grade variants the multi-chip package comes with a preconfigured heatspreader and the supplied metal heat slug is not required.

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. For more information concerning possible cooling solutions, see Table 4: Accessories.

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 10: Heatspreader Temperature Specification

Temperature Grade	Requirements
Commercial Grade	at 60°C HSP temperature on MCP @ 100% load needs to run at nominal frequency
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

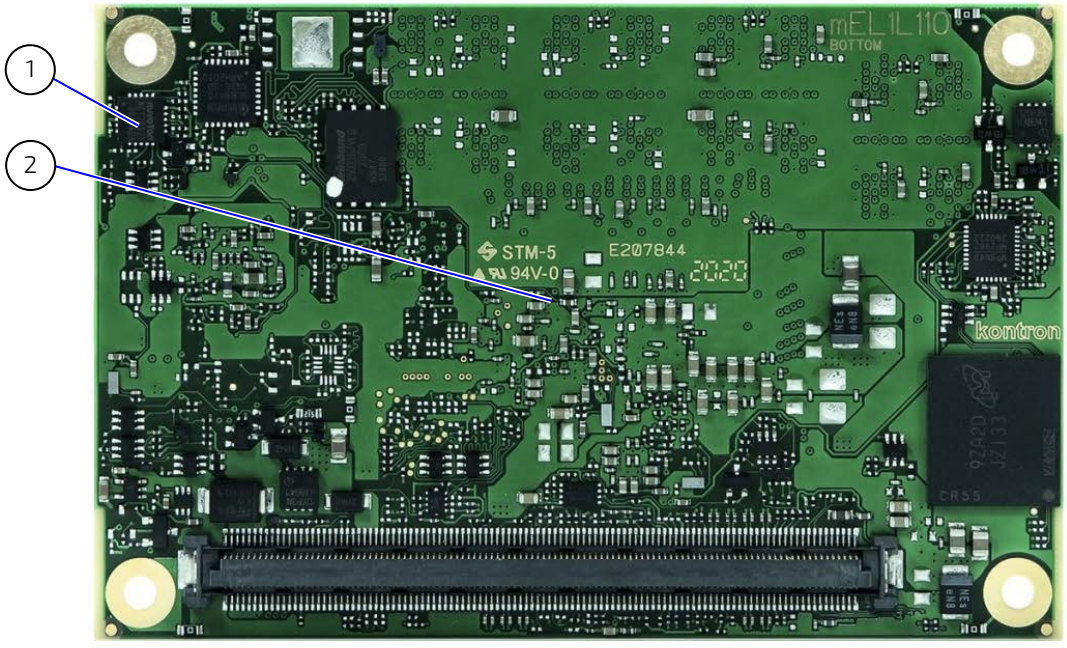
The operating temperature is the maximum measurable temperature on any spot on the module's surface.

2.5.5. Temperature Sensors

The thermal resistor (Figure 4,pos. 2) measures the Multi Chip Package (MCP) temperature. The thermal resistor is not capable of measuring very fast rises and falls in temperature and measurements may show a certain non-linearity. The thermal resistor gives a general indication of the ambient temperature close to the MCP. When comparing the thermal resistor value to the internal MCP values (i.e. DTS based values) differences are expected. These differences are due to the design and are not to be considered as an error. The MCP's temperature is referred to as CPU temperature in the BIOS set up menu: **Advanced> H/W Monitor> Reference Temperature**.

The on-module Hardware Monitor (HWM) chip uses an on-chip temperature sensor to measure the module's temperature and is referred to as module temperature in the BIOS set up menu: **Advanced>H/W Monitor> Reference Temperature**. The HWM uses the SMBus interface, see Table 20: SMBus Address.

Figure 4: Module Temperature Sensors

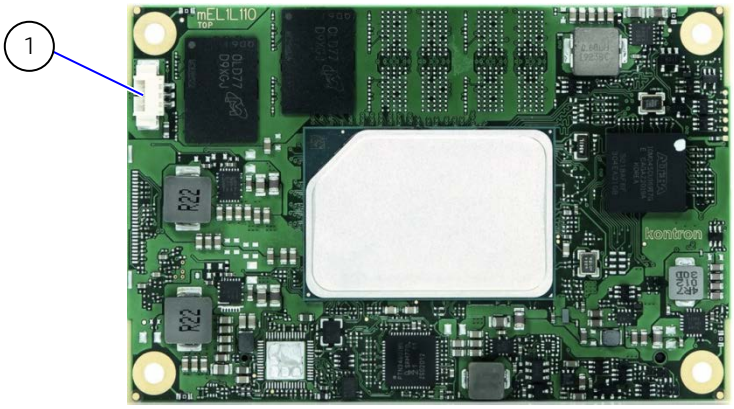


1	HWM measure the modules temperature	2	RT1- thermal resistor measures the MCP temperature

2.5.6. On-Module Fan Connector

The 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 11: 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-mEL10 supports two temperature grades commercial and Industrial (E2). The industrial temperature grade modules support an integrated heatspreader. For temperature grade information, see Chapter 2.1: Module Variants.

Table 12: Temperature Grades and Humidity Specification

Temperature Grades	Operating	Non-operating (Storage)
Commercial Grade	0°C to +60°C (32°F to 140°F)	-30°C to +85°C (-22°F to 185°F)
Industrial Grade (E2)	-40°C to +85°C (-40° to 185°F)	-40°C to +85°C (-40°F to 185°F
Relative Humidity	93 % , at +40°C, non-condensing	

2.7. Standards and Certifications

The COMe-mEL10 complies with the following standards and certificates. If modified, the prerequisites for specific approvals may no longer apply. For more information, contact Kontron Support.

Table 13: Standards and Certifications

EMC		
Emission	EN 55032 Class B CISPR32	Electromagnetic compatibility of multimedia equipment - Emission requirements
Immunity	IEC / EN 61000-6-2	Electromagnetic compatibility (EMC) Part 6-2: Generic standards - Immunity standard for industrial environments

Safety		
Europe	EN 62368-1	Safety for audio/video and information technology equipment
USA & Canada	UL 62368-1/CSA 62368-1 (Component Recognition)	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

Environment		
Shock	IEC / EN 60068-2-27	Non-operating shock test (half-sinusoidal, 11 ms, 15 g)
Vibration	IEC / EN 60068-2-6	Non-operating vibration (sinusoidal, 10 Hz – 2000 Hz, +/- 0.15 mm, 2 g)
RoHS II	Directive 2011/65/EU incl. 2015/863/EU	Restriction of Hazardous Substances in electrical and Electronic Equipment (RoHS)

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 calculations 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 14: MTBF

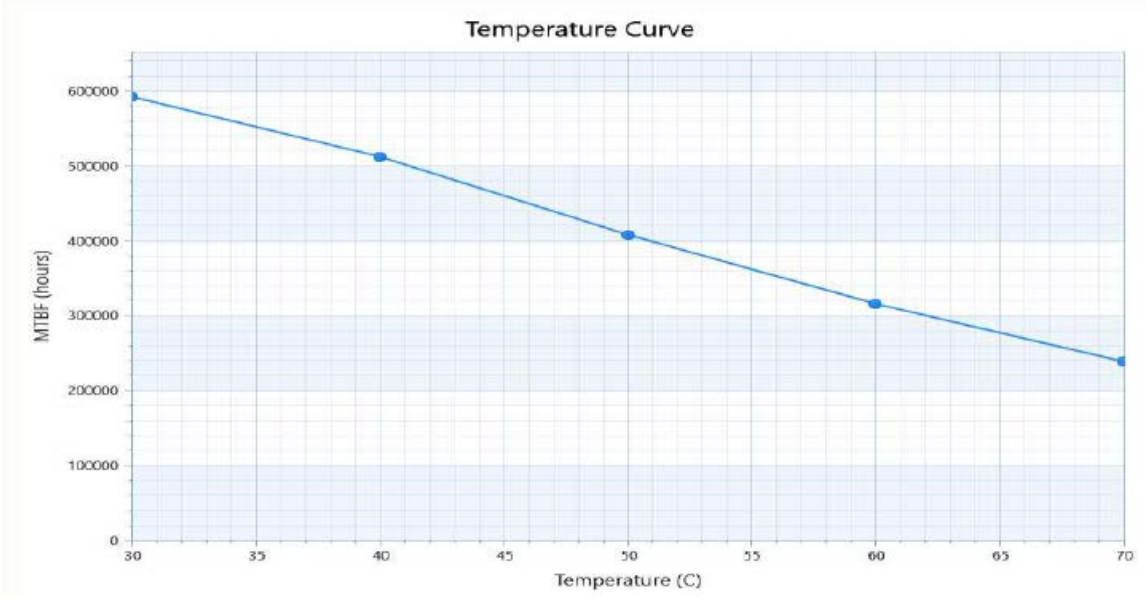
MTBF
System MTBF (hour) = 513232 h @ 40°C for COMe-mEL10 J6426 Reliability report article number: 34012-0432-J2-4
System MTBF (hour) = 508437 h @ 40°C for COMe-mEL10 E2 x6425RE Reliability report article number: 34013-0832-R2-4

The MTBF estimated value 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.

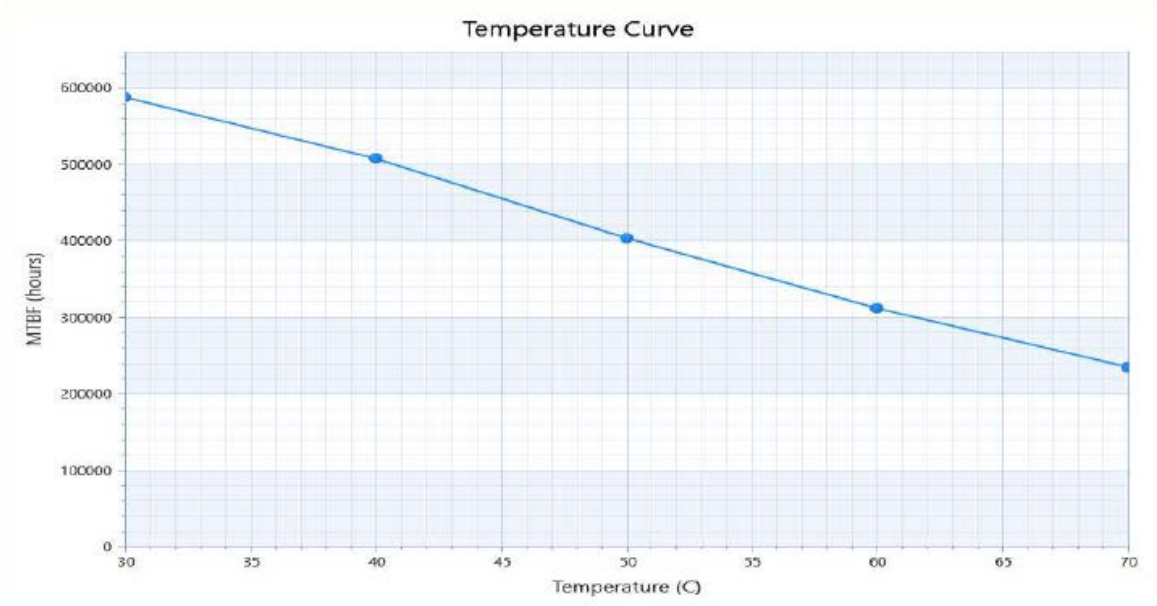
Figure 6 shows MTBF de-rating values for the commercial temperature range when used in an office or telecommunications environment. Other environmental stresses (extreme altitude, vibration, salt-water exposure, etc.) lower MTBF values.

Figure 6: MTBF De-rating Values

COMe-mEL10 J6426



COMe-mEL10 E2 x6425RE



2.8. Mechanical Specification

The COMe-mEL10 is compliant with the COM Express® PICMG COM.0 Rev 3.0 mechanical specification.

2.8.1. Module Dimensions

The mini module dimensions are 84 mm x 55 mm (3.3“ x 2.17“).

Figure 7: Module Dimensions

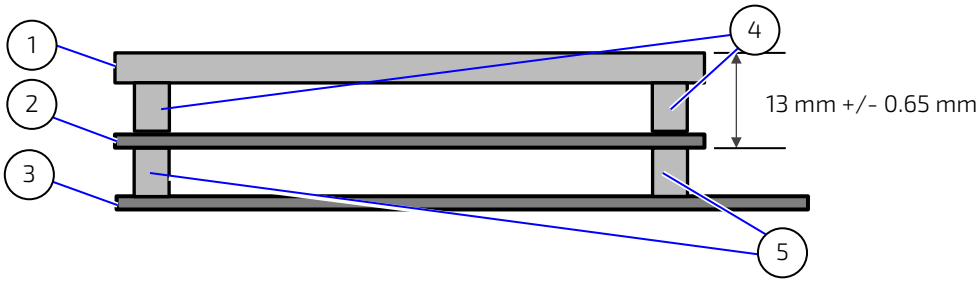
*All dimensions are in mm.

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 8.

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 8: Module and Carrier Height

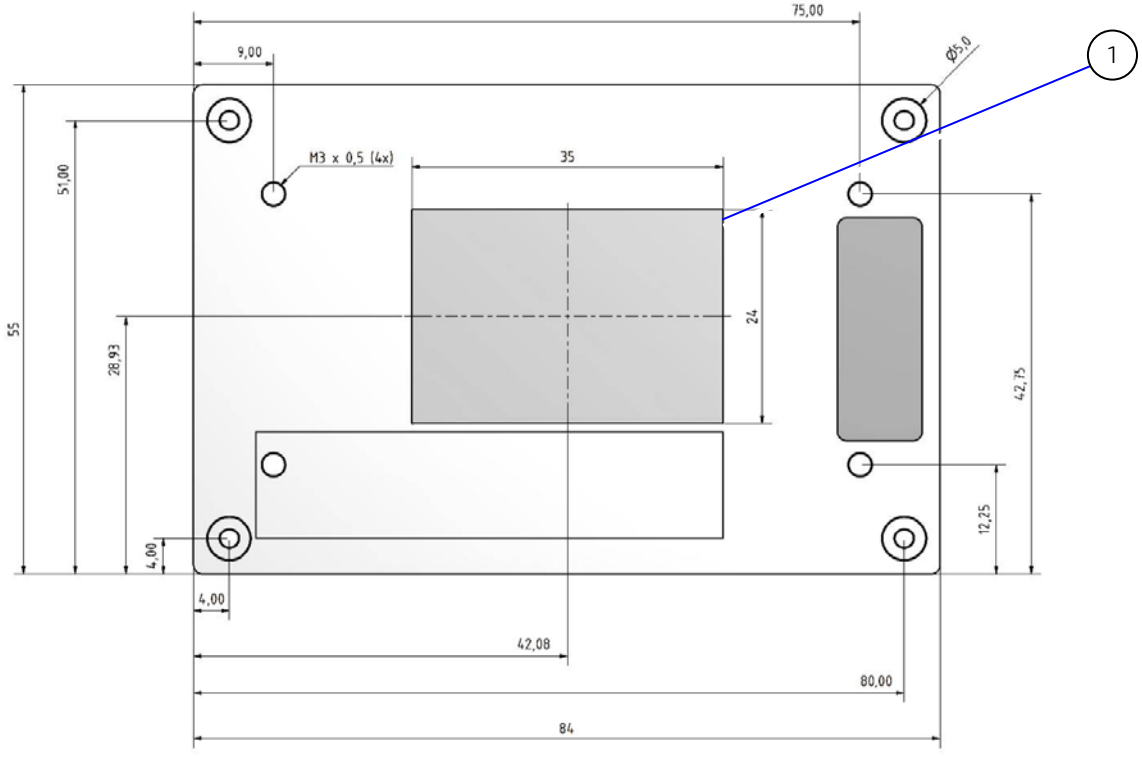


1	Heatspreader	4	Heatspreader standoff(s)
2	Module PCB board	5	Connector standoff(s) 5 mm or 8 mm
3	Carrier PCB board	6	13 mm +/- 0.65 mm

2.8.3. Metal Heat Slug Dimensions

The metal heat slug 35 mm x 24 mm (1.38" x 0.94") is located on top of the multi-chip package.

Figure 9: Metal Heat Slug Dimensions



*All dimensions shown in mm.

1	Metal heat slug

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-mEL10 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 S1.

Table 15: 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)

3.2. eMMC Flash Memory (option)

The Embedded Multimedia Flash Card (eMMC) is eMMC 5.1 compatible. The standard COMe-mEL10 variants support MLC. On request, eMMC pSLC can be offered. During the manufacturing process, Multi Level Cell (MLC) eMMC is reconfigured to act as pseudo Single Level Cell (pSLC) eMMC to provide improved reliability, endurance and performance.

The COMe-mEL10's eMMC flash memory supports up to 64 GByte pSLC or 128 GByte MLC.

3.3. eSPI Mode (option)

The eSPI interface is pin shared with LPC Interface signals to switch from one interface to another, a hardware modification in the form of additional resistors is required. The module's signal ESPI_EN# on pin B47 indicates whether ESPI-mode or LPC-mode is enabled/disabled. The LPC interface is the default connection to 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.

3.4. Fast I2C

The fast I2C bus transfer data between components on the same module with transfers at up to 400 kHz clock speeds.

The I2C controller supports:

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

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.

3.5. GPIO

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

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

The COMe-mEL10's GPIO pins are pin shared with SDIO pins. GPIO is the default and SDIO an option supported using the processor. Hardware assembly defines whether the shared pins are GPIO or SDIO. There is no BIOS or software option to change the shared pins.

Configuration must be performed using the OS driver.

3.6. Hardware Monitor (HWM)

The Hardware Monitor (HWM) Nuvoton NCT7802Y controls the health of the module by monitoring critical aspects such as the module's processor temperature using thermal resistors, power supply voltages and fan speed for cooling.

The SMART FAN ™ technology controls the duty cycle of the fan output (FAN_PWMOUT) with temperature setting points. This enables flexible fan control for cooling solutions and noise sensitive solutions. For system protection, users can set threshold values for alarm signals.

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

The HMW bus address is 5Ch.

3.7. LPC

The Low Pin Count (LPC) interface is pin shared with eSPI. The LPC is the default connection to the COMe connector. The signal pin B47 (ESPI_EN#) indicates whether ESPI-mode or LPC-mode is enabled/disabled.

In LPC mode "ESPI_EN#" is not connected 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.

The LPC low speed interface can be used for peripheral circuits such as an external Super I/O controller that typically combines legacy-device support into a single IC. The implementation of this subsystem complies with the COM Express® Specification. For more information, refer to the COM Express® Design Guide maintained by PICMG or the official PICMG documentation.

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

For LPC Super I/O, additional BIOS implementations are necessary, contact Kontron Support.

3.8. Intel® PSE

The Intel® Programmable Service Engine (PSE) is a dedicated offload engine for IoT functions such as embedded controller, low DMIP computing, network proxy, out-of-band device management, network proxy, real-time and sensor hub.

The COMe-mEL10 supports Intel® PSE. For more information, see Table 5: Processor Specification.

3.9. Intel® TCC

Intel® Time Coordinate Computing (TCC) improves the time synchronization performance and the timeless (also known as real-time) performance by providing a common timekeeping framework, making it possible for software to calculate the precise time between numerous systems.

The COMe-mEL10 supports Intel® TCC on industrial grade modules. For more information, see Table 5: Processor Specification.

3.10. Real Time Clock

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

The RTC's battery voltage range is 2.8 V to 3.47 V. Typical RTC values are 3 V and less than 10 µA. If the module is powered by mains supply, the RTC voltage is generated by on-module regulators, to reduce RTC current draw.

The COMe-mEL10 supports an internal RTC by default with the option for an external RTC on request.

Using the COMe-mEL10 without RTC battery voltage supply may result in improper behavior. Contact Kontron Support in case you plan a carrier design without RTC battery.

3.11. SDIO (option)

The SDIO features is supported from the processor. To find out more about SDIO, contact Kontron Support.

3.12. Serial Peripheral Interface (SPI)

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

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

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

3.12.1. SPI Boot

The SPI Flash chip stores the BIOS to be booted. The COMe-mEL10 supports SPI boot from the 32 MByte SPI Flash chip on the module and an external 32 MByte SPI Flash chip on a carrier board. The pins A34 (BIOS_DIS0#) and pin B88 (BIOS_DIS1#) select the SPI Flash boot source, see Table 16: SPI Boot Pin Configuration.

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

Table 16: SPI Boot Pin Configuration

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

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

Table 17: Supported SPI Boot Flash Types for 8-WSOIC Package

Size	Manufacturer	Part Number	Device ID
32MB	Winbond	W25Q256JV	EFh / 40h / 19h
32MB	Macronix	MX25L25645GZ2I	C2h / 20h / 19h
32MB	Micron	MT25QL256ABA1EW9-0SIT	20h / BAh / 19h
32MB	Cypress	S25FL256LAGNFI010	01h / 60h / 19h

3.12.2. 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 32MByte (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 command line.
In case of change, check Kontron's Customer Section for the latest BIOS binary package with reference command line.

3.12.3. 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.

3.13. 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-mEL10 supports firmware TPM (fTPM) using the integrated TPM 2.0 capability of the Intel Platform Trusted Technology (Intel® PTT). Hardware TPM is an option.

3.14. UART (option)

The UART serial communications interface option supports up to two serial RX/TX ports defined in the COMe specification on pins A98 (SER0_TX) and A99 (SER0_RX) for UART0, and pins A101 (SER1_TX) and A102 (SER1_RX) for UART1.

The UART option is 16550 compatible and features:

- 64-byte TX /RX host controller FIFOs
- On-chip bit rate (baud rate) generator
- Prioritized interrupt identification
- Programmable FIFO enable/disable

3.15. 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-mEL10 supports an independently programmable watchdog that works with two stages that can be used stage by stage.

Table 18: 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**	

3.15.1. Watchdog Timer Signal

The watchdog interrupt (WDT) on the COM Express® connector's pin B27 indicates a Watchdog time-out event. The WDT signal is configurable to any of the two stages. For more details, contact Kontron Support.

4/ System Resources

4.1. I2C Bus

The following table specifies the devices connected to the accessible I2C bus including the I2C address. The I2C bus is available at the COM Express® connector pin A83, I2C_CK and pin A84, I2C_DAT.

Table 19: I2C Bus Port Address

8-bit Address	7-bit Address	Used For	Available	Description
58h	2Ch	Internally reserved	No	
A0h	50h	Module EEPROM	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.

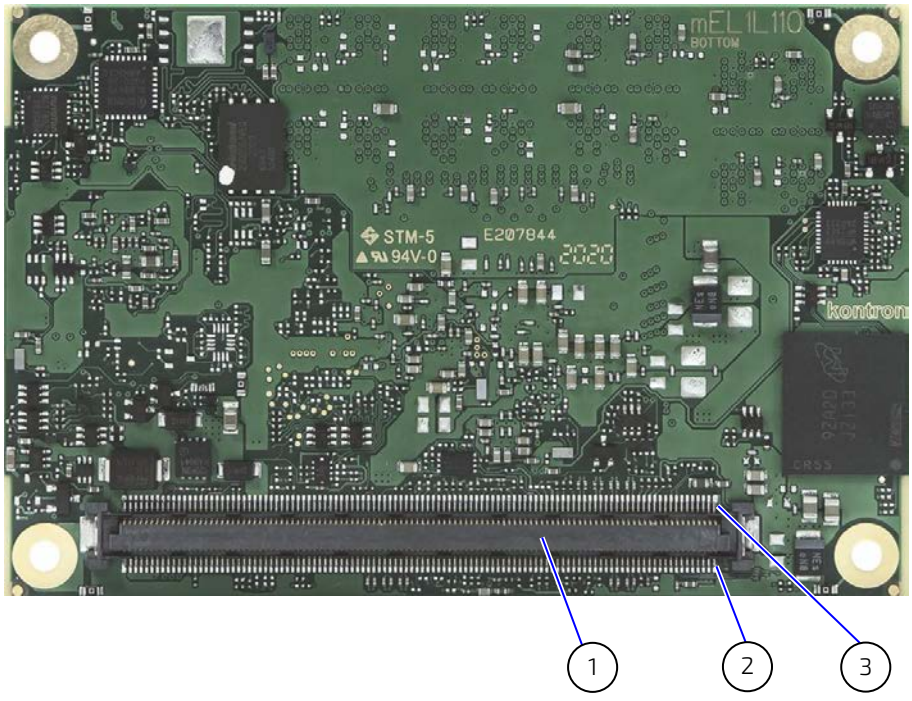
Table 20: SMBus Address

8-bit Address	7-bit Address	Device	Description
5Ch	2Eh	HWM NCT7802Y	Hardware Monitor. Do not use this address for external devices under any circumstances!

5/ COMe Interface Connector

The COMe interface connector (X1A) mounted on the bottom side of the module contains 220-pins with two rows where row A contains pins A1 to A110 and row B contains pins B1 to B110.

Figure 10: COMe Interface Connector



1	COMe interface connector (X1A)	3	X1A, Pin B1
2	X1A, Pin A1		

5.1. Connecting COMe Interface Connector to Carrier Board

The COMe interface connector (X1A), is inserted into the corresponding connector 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 Signals

The terms used in the connector pin assignment tables and a description of the signal type can be found in Table 21: General Signal Description. If additional information is required refer to the Appendix at the end of this user guide and the PICMG specification COM.0 Rev 3.0 Type 10 standard.

The information provided under type, module terminations and comments is complimentary to the COM.0 Rev 3.0 Type 10 standard. For more information, contact Kontron Support.

Table 21: 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	PD	Pull-Down Resistor
OD	Output Open Drain	PDS	Pull-Down-Strap
+ and -	Differential Pair Differentiator	PWR	Power Connection
		PWR GND	Power Ground Connection

5.3. COMe Interface Connector (X1A) Pin Assignment

The following tables list the pin assignment of the 220-pin COMe interface connector X1A (Row A1 to A110) and (Row B1 to B110).

5.3.1. Connector X1A Row A1 - A110

Table 22: Connector X1A Row A1 to A110 Pin Assignment

Pin	COMe Signal	Description	Type	Termination	Description
A1	GND	Power Ground	PWR GND		
A2	GBE0_MDI3-	Ethernet Media Dependent Interface 3	DP-I/O		
A3	GBE0_MDI3+				
A4	GBE0_LINK100#	Ethernet speed LED indicator	OD		
A5	GBE0_LINK1000#				
A6	GBE0_MDI2-	Ethernet Media Dependent Interface 2	DP-I/O		
A7	GBE0_MDI2+				
A8	GBE0_LINK#	Ethernet link LED indicator (LED)	OD		
A9	GBE0_MDI1-	Ethernet Media Dependent Interface 1	DP-I/O		
A10	GBE0_MDI1+				
A11	GND	Power Ground	PWR GND		
A12	GBE0_MDI0-	Ethernet Media Dependent Interface 0	DP-I/O		
A13	GBE0_MDI0+				
A14	GBE0_CTREF	Center Tab Reference Voltage	O		100 nF capacitor to GND
A15	SUS_S3#	Indicates Suspend to RAM (or deeper)	O-3.3	PD 10 kΩ	
A16	SATA0_TX+	SATA transmit data pair 0	DP-O	AC Coupled on Module	
A17	SATA0_TX-				
A18	SUS_S4#	Indicates Suspend to Disk (or deeper) state	O-3.3	PD 10 kΩ	
A19	SATA0_RX+	SATA receive data pair 0	DP-I	AC Coupled on Module	
A20	SATA0_RX-				
A21	GND	Power Ground	PWR GND		
A22	USB_SSRX0-	USB super speed receive data pair 0	DP-I		
A23	USB_SSRX0+				
A24	SUS_S5#	Indicates system is in Soft Off state	O-3.3	PD 10 kΩ	
A25	USB_SSRX1-	USB super speed receive data pair 1	DP-I		
A26	USB_SSRX1+				
A27	BATLOW#	Provides a battery-low signal to the module to indicate external battery is low	I-3.3	PU 10 kΩ, 3.3 V (S5)	Assertion prevents wake from S3-S5 state
A28	ATA_ACT#	Serial ATA activity LED indicator	OD-3.3	PU 10 kΩ, 3.3 V (S0)	Can sink 15 mA
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_CLK	HD Audio Bit Clock Output	O-3.3		
A33	HDA_SDOUT	HD Audio Serial Data Out	O-3.3		
A34	BIOS_DIS0#	BIOS selection straps 0	I-3.3	PU 10 kΩ, 3.3 V (S5)	

Pin	COMe Signal	Description	Type	Termination	Description
A35	THRMTRIP#	Thermal Trip indicates CPU has entered thermal shutdown	O-3.3 OD	PU 10 kΩ, 3.3 V (S0)	Thermal trip event transition to S5 indicator
A36	USB6-	USB 2.0 data differential pair port 6	DP-I/O	PD 14.25 KΩ to 14.8 kΩ in PCH	
A37	USB6+				
A38	USB_6_7_OC#	USB overcurrent indicator port 6/7	I-3.3	PU 10 kΩ, 3.3 V (S5)	
A39	USB4-	USB 2.0 data differential pair port 4	DP-I/O	PD 14.25 KΩ to 14.8 kΩ in PCH	
A40	USB4+				
A41	GND	Power Ground	PWR GND		
A42	USB2-	USB 2.0 data differential pair port 2	DP-I/O	PD 14.25 KΩ to 14.8 kΩ in PCH	
A43	USB2+				
A44	USB_2_3_OC#	USB overcurrent indicator port 2/3	I-3.3	PU 10 kΩ, 3.3V (S5)	
A45	USB0-	USB 2.0 data differential pairs port 0	DP-I/O	PD 14.25 KΩ to 14.8 kΩ in PCH	
A46	USB0+				
A47	VCC_RTC	Real Time Clock (RTC) circuit power input	PWR 3V		Voltage range 2.8 V to 3.47 V
A48	RSVD	Reserved for future use	NC		
A49	GBE0-SDP	Gigabit Ethernet Controller 0 Software-Definable pin	I/O-3.3	PD 10 kΩ	
A50	LPC_SERIRQ / ESPI_CS1#	Serial interrupt request / eSPI master Chip select 1	I/OD-3.3 / O-1.8	PU 8.2 kΩ, 3.3 V (S0) / -	
A51	GND	Power Ground	PWR GND		
A52	RSVD	Reserved for future use	NC		
A53	RSVD				
A54	GPI0	General purpose input 0	I-3.3	PU 100 kΩ, 3.3 V (S0)	Option SD_DATA0
A55	RSVD	Reserved for future use	NC		
A56	RSVD				
A57	GND	Power Ground	PWR GND		
A58	PCIE_TX3+	PCI Express transmit lane 3	DP-O	AC Coupled on Module	
A59	PCIE_TX3-				
A60	GND	Power Ground	PWR GND		
A61	PCIE_TX2+	PCI Express transmit lane 2	DP-O	AC Coupled on Module	
A62	PCIE_TX2-				
A63	GPI1	General purpose input 1	I-3.3	PU 100 kΩ, 3.3 V (S0)	Option SD_DATA1
A64	PCIE_TX1+	PCI Express transmit lane 1	DP-O	AC Coupled on Module	
A65	PCIE_TX1-				
A66	GND	Power Ground	PWR GND		
A67	GPI2	General purpose input 2	I-3.3	PU 100 kΩ, 3.3 V (S0)	Option SD_DATA2
A68	PCIE_TX0+	PCI Express transmit lane 0	DP-O	AC Coupled on Module	
A69	PCIE_TX0-				
A70	GND	Power Ground	PWR GND		

Pin	COMe Signal	Description	Type	Termination	Description
A71	LVDS_A0+	LVDS channel A DAT0 or EDP Lane 2 transmit	DP-O		Optional EDP_TX2+
A72	LVDS_A0-				Optional EDP_TX2-
A73	LVDS_A1+	LVDS channel A DAT1 or EDP Lane 1 transmit	DP-O		Optional EDP_TX1+
A74	LVDS_A1-				Optional EDP_TX1-
A75	LVDS_A2+	LVDS channel A DAT2 or EDP Lane 0 transmit	DP-O		Optional EDP_TX0+
A76	LVDS_A2-				Optional EDP_TX0-
A77	LVDS_VDD_EN	LVDS or EDP panel power control	O-3.3	PD 100 kΩ	Optional EDP_VDD_EN
A78	LVDS_A3+	LVDS channel A DAT3	DP-O		
A79	LVDS_A3-				
A80	GND	Power Ground	PWR GND		
A81	LVDS_A_CK+	LVDS channel A clock or EDP lane 3 transmit	DP-O		Clock 20 MHz to 80 MHz Option EDP_TX3-
A82	LVDS_A_CK-				
A83	LVDS_I2C_CK	LVDS I2C Clock for (DDC) / eDP AUX +	I/O-3.3	PU 2.2 kΩ, 3.3 V (S0)	Optional EDP_AUX+
A84	LVDS_I2C_DAT	LVDS I2C Data (DDC) / eDP AUX -	I/O-3.3	PU 2.2 kΩ, 3.3 V (S0)	Optional EDP_AUX-
A85	GPI3	General purpose input 3	I-3.3	PU 100 kΩ 3.3V (S0)	Option SD_DATA3
A86	RSVD	Reserved for future use	NC		
A87	eDP_HPD	Detection of Hot Plug / Unplug	I-3.3	PD 400 kΩ LVDS / 100 kΩ EDP	
A88	PCIE_CK_REF+	Reference PCI Express Clock for all PCI Express and PCI Express Graphics lanes	DP-O		100 MHz
A89	PCIE_CK_REF-				
A90	GND	Power Ground	PWR GND		
A91	SPI_POWER	3.3 V Power Output for external SPI Flash	O-3.3		100 mA maximum
A92	SPI_MISO	Data in to module from carrier SPI (SPI Master IN Slave Out)	I-3.3		
A93	GPO0	General purpose output 0	O-3.3	PD 100 kΩ	Optional SD_CLK
A94	SPI_CLK	SPI clock Clock from Module to Carrier SPI	O-3.3		
A95	SPI_MOSI	SPI master Out Slave In Data out from Module to Carrier SPI	O-3.3		
A96	TPM_PP	TPM physical presence	I-3.3	PD 4.7 kΩ	TMP does not use this functionality
A97	TYPE10#	Indicates to Carrier Board that type 10 module is installed	PDS	PD 47 kΩ	
A98	SER0_TX	Serial port 0 TXD	O-3.3		20 V protection circuit implemented on-module, PD on carrier boards needed for proper operation
A99	SER0_RX	Serial port 0 RXD	I-5T	PU 47 kΩ, 3.3 V (S0)	20 V protection circuit implemented on-module
A100	GND	Power Ground	PWR GND		
A101	SER1_TX	Serial port 1 TXD	O-3.3		20 V protection circuit implemented on-module, PD on carrier boards needed for proper operation

Pin	COMe Signal	Description	Type	Termination	Description
A102	SER1_RX	Serial port 1 RXD	I-5T	PU 47 kΩ, 3.3 V (S0)	20 V protection circuit implemented on-module
A103	LID#	LID switch input	I-3.3	PU 47 KΩ, 3.3 V (S5)	
A104	VCC_12V	Main input voltage (4.75 V to 20 V)	PWR 4.75 V to 20 V		
A105	VCC_12V				
A106	VCC_12V				
A107	VCC_12V				
A108	VCC_12V				
A109	VCC_12V				
A110	GND	Power Ground	PWR GND		

+ and - Differential pair differentiator

5.3.2. Connector X1A Row B1 – B110

Table 23: Connector X1A Row B1 to B110 Pin Assignment

Pin	COMe Signal	Description	Type	Termination	Description
B1	GND	Power Ground	PWR GND		
B2	GBE0_ACT#	Ethernet Controller activity LED indicator	OD		
B3	LPC_FRAME# / ESPI_CS0	Indicates start of LPC Frame	O-3.3 / O-1.8		
B4	LPC_AD0 / ESPI_IO_0	LPC multiplexed command, address and data bus 0 / eSPI Master data I/O 0	I/O-3.3	PU 20 KΩ 3.3 V (S0)	PU only for LPC option
			1/O-1.8		
B5	LPC_AD1 / ESPI_IO_0	LPC multiplexed command, address and data bus 1 / eSPI Master data I/O 1	I/O-3.3	PU 20 KΩ 3.3 V (S0)	
B6	LPC_AD2 / ESPI_IO_2	LPC multiplexed command, address and data bus 2 / eSPI Master data I/O 2	I/O-3.3	PU 20 KΩ 3.3 V (S0)	
B7	LPC_AD3 / ESPI_IO_3	LPC multiplexed command, address and data bus 3 / eSPI Master data I/O 3	I/O-3.3 /	PU 20 KΩ 3.3 V (S0)	
B8	LPC_DRQ0# / ESPI_ALERT0	LPC serial DMA master request	I-3.3 / I-1.8	PU10 KΩ 3.3 V / PU 1 kΩ 1.8 V	LPC DMA request not supported
B9	LPC_DRQ1#/ ESPI_ALERT1		I-3.3 / I-1.8	PU10 KΩ 3.3 V / PU 1 kΩ 1.8 V	
B10	LPC_CLK/ ESPI_CK	LPC 25 MHz clock output	O-3.3 / O-1.8		25 MHz (LPC) 20 MHz (eSPI)
B11	GND	Power Ground	PWR GND		
B12	PWRBTN#	Power Button event	I-3.3	PU 10 kΩ, 3.3 V (S5)	Brings a system out of S5 soft-off and other suspend states, and powers the module down.
B13	SMB_CLK	SMBus clock line	O-3.3	PU 10 kΩ 3.3 V (S5)	

Pin	COMe Signal	Description	Type	Termination	Description
B14	SMB_DAT	SMBus bidirectional data line	I/O-3.3	PU 3.74 kΩ 3.3 V (S5)	
B15	SMB_ALERT#	SMBus alert generates a SMI# or wakes the system	I-3.3	PU 10 kΩ, 3.3 V (S5)	
B16	SATA1_TX+	SATA transmit data pair 1	DP-O	AC Coupled on Module	
B17	SATA1_TX-				
B18	SUS_STAT# / ESPI_RESET	Suspend status / eSPI Reset	O-3.3 / O-1.8	PD 10 kΩ / PD 76.8 kΩ	Notifies LPC devices of. imminent suspend / -
B19	SATA1_RX+	SATA receive data pair 1	DP-I	AC Coupled on Module	
B20	SATA1_RX-				
B21	GND	Power Ground	PWR GND		
B22	USB_SSTXO-	USB super speed transmit pair 0	DP-O		
B23	USB_SSTX0+				
B24	PWR_OK	Power OK from main power supply	I-5T	PU 51 kΩ, 3.3 V	20 V protection circuit implemented on module
B25	USB_SSTX1-	USB super speed transmit pair 1	DP-0		
B26	USB_SSTX1+				
B27	WDT	Indicates watchdog time-out event has occurred	O-3.3	PD 10 kΩ	
B28	HDA_SDIN2	Audio Codec serial data input 2	I-3.3	NC	Not supported
B29	HDA_SDIN1	Audio Codec serial data input 1	I-3.3		
B30	HDA_SDIN0	Audio Codec serial data input 0	I-3.3		
B31	GND	Power Ground	PWR GND		
B32	SPKR	Speaker output provides the PC beep signal and is mainly intended for debugging purposes	O-3.3	PD 20 kΩ in PCH	PD is removed after reset is de-asserted
B33	I2C_CK	I2C port clock output	O-3.3	PU 2.21 kΩ 3.3 V (S5)	
B34	I2C_DAT	I2C port data I/O line	I/O-3.3		
B35	THRM#	Input from off-module temp sensor indicating an over-temp situation	I-3.3	PU 10 kΩ, 3.3 V (S0)	
B36	USB7-	USB 2.0 differential data pairs port 7	DP-I/O	PD 14.25 kΩ to 24.8 kΩ	
B37	USB7+				
B38	USB_4_5_OC#	USB overcurrent indicator port 4/5	I-3.3	PU 10 kΩ, 3.3 V (S5)	
B39	USB5-	USB 2.0 differential data pairs port 5	DP-I/O	PD 14.25 kΩ to 24.8 kΩ	
B40	USB5+				
B41	GND	Power Ground	PWR GND		
B42	USB3-	USB 2.0 differential data pairs port 3	DP-I/O	PD 14.25 kΩ to 24.8 kΩ	
B43	USB3+				
B44	USB_0_1_OC#	USB overcurrent indicator port 0/1	I-3.3	PU 10 KΩ, 3.3 V (S5)	
B45	USB1-	USB 2.0 differential data pairs port 1	DP-I/O	PD 14.25 kΩ to 24.8 kΩ	
B46	USB1+				
B47	ESPI_EN#	Enable/disable ESPI-mode/LPC-mode	I-3.3	PU 10 kΩ 3.3 V (S5)	
B48	USB0_HOST_PRSNT	USB Host present on USB0	I-3.3	PD 100 KΩ	

Pin	COMe Signal	Description	Type	Termination	Description
B49	SYS_RESET#	Reset button input	I-3.3	PU 10 kΩ, 3.3 V (S5)	
B50	CB_RESET#	Carrier board reset	O-3.3	PD 10KΩ	Resets output from module to carrier board
B51	GND	Power Ground	PWR GND		
B52	RSVD	Reserved for future use	NC		
B53	RSVD				
B54	GPO1	General purpose output 1	O-3.3	PD 100 kΩ	Optional SD_CMD
B55	RSVD	Reserved for future use	NC		
B56	RSVD				
B57	GPO2	General purpose output 2	O-3.3	PD 100 KΩ	Optional SD_WP
B58	PCIE_RX3+	PCI Express receive lane 3	DP-I		
B59	PCIE_RX3-				
B60	GND	Power Ground	PWR		
B61	PCIE_RX2+	PCI Express receive lane 2	DP-I		
B62	PCIE_RX2-				
B63	GPO3	General purpose output 3	O-3.3	PD 100 KΩ	Optional SD_CD#
B64	PCIE_RX1+	PCI Express receive lane 1	DP-I		
B65	PCIE_RX1-				
B66	WAKE0#	PCI Express Wake Event, wake up signal	I-3.3	PU 10 KΩ, 3.3 V (S5)	
B67	WAKE1#	General purpose Wake Event	I-3.3	PU 10 KΩ, 3.3 V (S5)	Implement on PS2 keyboard or mouse
B68	PCIE_RX0+	PCI Express receive lane 0	DP-I		
B69	PCIE_RX0-				
B70	GND	Power Ground	PWR GND		
B71	DDI0_PAIR0+	DDIO data pair 0	DP-O		
B72	DDI0_PAIR0-				
B73	DDI0_PAIR1+	DDIO data pair 1	DP-O		
B74	DDI0_PAIR1-				
B75	DDI0_PAIR2+	DDIO data pair 2	DP-O		
B76	DDI0_PAIR2-				
B77	DDI0_PAIR4+	DDIO data pair 4	NC		Not supported
B78	DDI0_PAIR4-				
B79	LVDS/BKLT_EN	LVDS /EDP panel backlight enable (ON)	O-3.3	PD 100 kΩ	Optional EDP_BKLT_EN
B80	GND	Power Ground	PWR GND		
B81	DDI0_PAIR3+	DDIO data pair 3	DP-O		
B82	DDI0_PAIR3-				
B83	LVDS/BKLT_CTRL	LVDS / EDP panel backlight brightness control	O-3.3		Optional EDP_BKLT_CTRL
B84	VCC_5V_SBY	5V Standby	PWR 5 V (S5)		Optional, not necessary in single supply mode
B85	VCC_5V_SBY				
B86	VCC_5V_SBY				
B87	VCC_5V_SBY				
B88	BIOS_DIS1#	BIOS selection strap to determine BIOS boot device	I-3.3	PU 10 KΩ, 3.3 V (S5)	

Pin	COMe Signal	Description	Type	Termination	Description
B89	DDO_HPD	DDIO hot plug detect	I-3.3	PD 100 kΩ	
B90	GND	Power Ground	PWR GND		
B91	DDI0_PAIR5+	DDIO data pair 5	NC		Not supported
B92	DDI0_PAIR5-				
B93	DDI0_PAIR6+	DDIO data pair 6	NC		Not supported
B94	DDI0_PAIR6-				
B95	DDI0_DCC_AUX_SEL	DDIO DCC/ Aux select	I-3.3	PD 1 MΩ	
B96	USB_HOST_PRSNT	USB host preset on USB7	I-3.3	PD 100 kΩ	
B97	SPI_CS#	Chip select for carrier board SPI	0-3.3		
B98	DDI0_CTRLCLK_AUX+	DDIO auxiliary clock control signal	I/O-3.3	PD 100 kΩ	PU 2.2 kΩ if DCC is selected
B99	DDI0CTRLDATA_AUX-	DDIO auxiliary data control signal	I/O-3.3	Pu 100 kΩ, 3,3V (S0)	
B100	GND	Power Ground	PWR GND		
B101	FAN_PWMOUT	Fan speed control by PWM Output	0-3.3		20 V protection circuit implemented on module, PD on carrier board needed for proper operation.
B102	FAN_TACHIN	Fan tachometer input for fan with a two-pulse output	I-3.3	PU 47 kΩ, 3.3 V (S0)	20 V protection circuit implemented on module
B103	SLEEP#	Sleep button signal used by ACPI operating system to bring system to sleep state or wake it up again	I-3.3	PU 47 kΩ, 3.3 V (S5)	
B104	VCC_12V	Main input voltage (4.75 V-20 V)	PWR 4.75 V to 20 V		
B105	VCC_12V				
B106	VCC_12V				
B107	VCC_12V				
B108	VCC_12V				
B109	VCC_12V				
B110	GND	Power Ground	PWR GND		

+ and - Differential pair differentiator

6/ UEFI BIOS

6.1. Starting the uEFI BIOS

The COMe-mEL10 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 COMe-mEL10.

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 Menu), press <RETURN>, and proceed with step 5.
5. The setup menu appears.

6.2. Navigating the uEFI BIOS

The COMe-mEL10 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 24: Navigation Hot Keys Available in the Legend Bar

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

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 11: Setup Menu Selection Bar

The setup menus available for the COMe- mEL10 are:

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

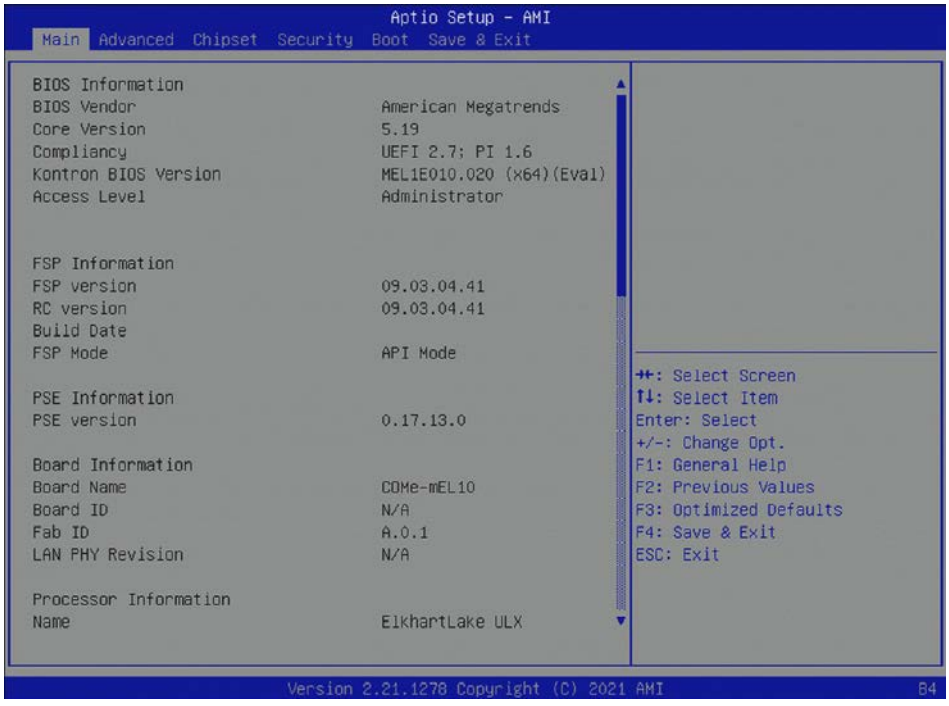
The currently active menu is highlighted in grey and the currently active uEFI BIOS setup item is highlighted in white. Use the left and right arrow keys to select the setup menu.

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.

6.4.1. Main Setup Menu

The Main setup menu lists sub-screens and second level sub-screens of the functions supported within the Main setup menu.

Figure 12: Main Setup Menu



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

Table 25: Main Setup Menu Sub-screens and Functions

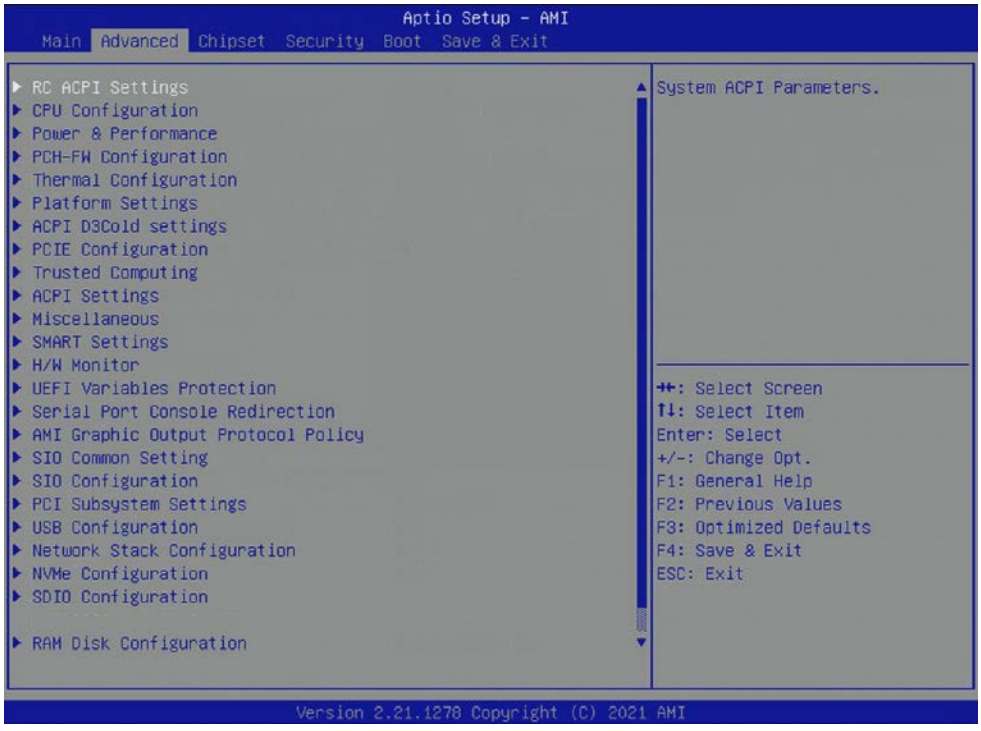
Sub-screen	Description
BIOS Information>	Read only field BIOS Information BIOS vendor, Core version, Compliancy, Project version, Access level, FSP information, Build date, Board information, Processor information, PCH information, Package type and Firmware version
System Language>	Choose the system default language: [**English**]
Platform Information>	Read only field Module Information Product name, Revision, Serial # ,MAC address, Boot counter, and CPLD rev
System Date>	Displays the system date [Week day mm/dd/yyyy]
System Time>	Displays the system time [hh:mm:ss]

6.4.2. Advanced Setup Menu

The Advanced Setup menu lists sub-screens and second level sub-screens of the functions supported within the Advanced setup menu.

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

Figure 13: Advanced Setup Menu



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

Table 26: Advanced Setup Menu Sub-screens and Functions

Sub-screen	Next Level Sub-screens / Description	
RC ACPI Settings>	Native PCIE Enable>	Bit - PCIE Native * Control 0.- hot plug 1. - SHPC native Hot plug control 2. - Power management 3. - PCIe Advanced 4 – PCIe capability structure control 5- Latency Tolerance reporting control [**Enabled**, Disabled]
	Native ASPM>	Enables – OS control Disabled – BIOS controlled ASPM [Enabled, **Disabled**]

Sub-screen	Next Level Sub-screens / Description		
RC ACPI Settings> (continued)	Wake System from S5 via RTC>	System wake on alarm event. When enabled system will wake on the hr:min::sec::specified [Enabled, **Disabled**]	
	Low Power S0 Idle Capability>	Determines If ACPI Lower power S0 idle capability (mutually exclusive with smart Connect). While enabled 8254 timer is disabled for SLP_S0 support. [Enabled, **Disabled**]	
	PCI Delay Optimization>	Experimental ACPI additions for FW latency optimization [Enabled, **Disabled**	
	MSI Enable>	MSI support is disables in FADT [**Enabled**, Disabled]	
Sub-screen	**Next level Sub-Screens / Description**		
CPU Configuration>	Read only field CPU Configuration: Type, IS, Speed, L1 Data Cache, L1 Instruction Cache, L2 Cache, L3 cache, L4 Cache, VMX, SMX/TXT		
	CPU Flex Ratio Override>	CPU flex ration programming [Enabled, **Disabled**]	
	CPU Flex Ratio Setting>	Read only field CPU Flex Ratio setting [**18**]	
	Hardware Prefetcher>	Turns on/OFF the MLC streamer prefetcher [**Enabled**, Disabled]	
	Adjacent Cache Line Prefetch>	Turns on/OFF prefetching of adjacent cache lines [**Enabled**, Disabled]	
	Intel (VMX) Virtualization Technology>	When enabled VMM can utilize the additional hardware capabilities provided by Vanderpool Technology. [**Enabled**, Disabled]	
	Active Processor Cores>	Number of core to enable in each processor package [**ALL**, 1, 2,3]	
	BIST>	Built-In Self-Test (BIST on reset) [Enabled, **Disabled**]	
	AP Threads Idle Manner>	AP threads idle manner for waiting signal to run [HALT loop, **MWAIT Loop**, RUN loop]	
	AES>	Advanced Encryption Standard [**Enabled**, Disabled]	
	Machine Check>	Machine Check [**Enabled**, Disabled]	
	Monitor MWait>	Monitor MWait [**Enabled**, Disabled]	
	CPU SMM Enhancement>	SMM use Delay Indication>	Uses of SMM_Delay MSR for MP sync in SMI [**Enabled**, Disabled]
		SMM use Block Indication>	Use of SMM_Blocked MSR for MP sync in SMI [**Enabled**, Disabled]
		SMM use SMM en-US Indication>	Uses of SMM_Enable MSR for MP sync in SMI [**Enabled**, Disabled]

Sub-screen	Next Level Sub-screens / Description			
Power and Perfomance>	CPU Power Management>	Read only field P1 to P3 Fused Max Core Ratio		
		Boot Performance Mode>	Select the performance state that the BIOS will set starting from rest vector. [Max Battery, **Max Non-Turbo Performance**, Turbo Performance]	
		Intel® Speedstep™>	Allows more than two frequency ranges to be support. [**Enabled**, Disabled]	
		Race to Halt>	RTH dynamically increases CPU frequency in order to enter pkg C-State faster to reduce overall power. (RTH controlled through MSR 1FC bit 20) [**Enabled**, Disabled]	
		Turbo Mode>	Processor turbo mode (requires EMTTM enabled too). Auto means enabled. [**Enabled**, Disabled]	
		View/Configure Turbo options>	Read only field Max/Min turbo limits, Package TDP limit, Power Limit 1 & 2, 1 to 4-Core Turbo Ratio	
			Energy Efficient P-State>	When set to 0: disables access to ENERGY_PERFORMANCE: BIAS MSR and CPUID function 6 ECX reads 0 indicating no support for energy efficient policy setting. When set to 1 : enables access to ENERGY PERFORANCE_BIAS MSR 1B0h and CPUID function 6 ECX[3] will read 1 indicating Energy Efficient Policy is supported. [**Enabled**, Disabled]
			Package Power Limits MSR Lock>	Enables PACAGE_POWER_LIMIT MSR locked and a reset required to unlock the register. [Enabled, **Disabled**]
			Power Limit 1 Override>	If disables: BIOS programs the default values for power limit 1 and power limit 1, time window. [Enabled, **Disabled**]
			Power Limit 2 Override>	If disables: BIOS programs the default values for power limit 2. [**Enabled**, Disabled]
			Power Limit 2>	Power limit 2 in mW When programming BIOS rounds to nearest 1/8W. If value is 0, BIOS programs this value as 1.25 x TDP. For 12.5W, enter 12500. [**0**]
			1-Core Ratio Limit Override>	Range 0 to 83. Minimum range varies between processors. This 1-Core ration limit must be greater than or equal to 2-Core/3-Core and 4-Core ratio limit. [**0**]

Sub-screen	Next Level Sub-screens / Description			
Power and Performance> (continued)	CPU Power Management> (continued)	View/Configure Turbo Options> (continued)	2-Core Ratio Limit Override>	Range 0 to 83. Minimum range varies between processors. This 2-Core ration limit must be less than or equal to 1-Core ratio limit. [**0**]
			3-Core Ratio Limit Override>	Range 0 to 83. Minimum range varies between processors. This 3-Core ration limit must be less than or equal to 1-Core ratio limit. [**0**]
			4-Core Ratio Limit Override>	Range 0 to 83. Minimum range varies between processors. This 4-Core ration limit must be less than or equal to 1-Core ratio limit. [**0**]
			Energy Efficient Turbo>	Lower frequency to increase efficiency. Disable only in overclocking situation where turbo frequency must remain constant. Otherwise, leave enabled. [**Enabled**, Disabled]
		Platform PL1 Enable>	Platform power limit programming. Enable activated the PL1 value to be used by the processor to limit the average power of given time window. [Enabled, **Disabled**]	
		Platform PL2 Enable>	Platform power limit programming. If disabled BIOS programs the default value for platform Power Limit2 [Enabled, **Disabled**]	
		Power Limit 4 Override>	If disable BIOS will leave the default values for power limit 4. [Enabled, **Disabled**]	
		C-states	Allows CPU to go to c-states when not 100 utilized [**Enabled**, Disabled]	
		Enhanced C-States>	CPU switches to minimum speed when all cores enter c-state. [**Enabled**, Disabled]	
		C-states Auto Demotion>	Configure c-state Auto demotion [Disabled, **C1**]	
		C-states UN-demotion>	Configure c-state un-demotion [Disabled, **C1**]	
		Package C-state demotion>	Package c-state demotion [**Enabled**, Disabled]	
		Package C-state un-demotion>	Package c-state un-demotion [**Enabled**, Disabled]	
		C-State Pre-wake>	Disables sets bit 30 of Power-CTL MSR(0x1FC) to 1 to disable the c-state pre-wake. [**Enabled**, Disabled]	
		IO MWait Redirection>	Enable: mapa IO read instructions sent to IO registers PMG_IO_BASE_ADDRBASE+off set to MWait (offset) [Enabled, **Disabled**]	

Sub-screen	Next Level Sub-screens / Description			
Power and Performance> (continued)	CPU Power Management> (continued)	Package C-State Limit>	Maximum c-state limit setting. CPU Default: leaves factory default Auto: initializes to deepest available c state limit [C0/C1, C2, C3, **C6**, C7, C8, C9, C10, CPU Default, Auto]	
		C6/C7 Short Latency Control (MSR 0x60B)		
		Time Unit>	Unit of measurement for IRTL value bits [12:10) [1ns, 32ns, **1024ns**, 32768ns, 1048576ns, 33554432ns]	
		Latency>	Interrupt response time limit value bits [9:0] Enter 0 to 1023. [**0**]	
		C6/C7 Long latency Control (MSR 0x60C)		
		Time Unit>	Unit of measurement for IRTL value bits [12:10]. [1ns, 32ns, **1024ns**, 32768ns, 1048576ns, 33554432ns]	
		Latency>	Interrupt response time limit value- bits [9:0] Enter 0 to 1023. [**0**]	
		C8 Latency Control (MSR 0x633)		
		Time Unit>	Unit of measurement for IRTL value bits [12:10) [1ns, 32ns, **1024ns**, 32768ns, 1048576ns, 33554432ns]	
		Latency>	Interrupt response time limit value- bits [9:0] Enter 0 to 1023. [**0**]	
		C9 Latency Control (MSR 0x634)		
		Time Unit>	Unit of measurement for IRTL value bits [12:10) [1ns, 32ns, **1024ns**, 32768ns, 1048576ns, 33554432ns]	
		Latency>	Interrupt response time limit value- bits [9:0] Enter 0 to 1023. [**0**]	
		C10 Latency Control (MSR 0x635)		
		Time Unit>	Unit of measurement for IRTL value bits [12:10) [1ns, 32ns, **1024ns**, 32768ns, 1048576ns, 33554432ns]	
		Latency>	Interrupt response time limit value bits [9:0] Enter 0 to 1023.[**0**]	
		Thermal Monitor>	Enable or disable the thermal monitor [**Enabled**, Disabled]	
		Interrupt redirection Mode Selection>	Selects the logical interrupts [**Fixed Priority**, Round Robin, Hash vector, No Change]	
		Timed MWAIT>	Enable or disables the timed MWait support [Enabled, **Disabled**]	
		Custom P-State Table>	Sets the number of customer P-states. At least 2 states must be present. [**0**]	
		Power Limit 3 Settings>	Read only field	
		CPU Lock Configuration>	CFG Lock>	Configure MSR 0xE2[15], CFG lock bit [**Enabled**, Disabled]

Sub-screen	Next Level Sub-screens / Description			
Power and Performance> (continued)	CPU Power Management> (continued)	CPU Lock Configuration> (continued)	Overclocking Lock>	Over clocking lock (Bit 20) in FLEX_Ratio (194) MSR [Enabled, **Disabled**]
	GT- Power Management Control>	RC6 (Render Standby)>	Checks Enable render standby support [**Enabled**, Disabled]	
		Maximum GT Frequency>	Maximum GT frequency limited by user Choose between 200 MHz (RPN) and 850 MHz (RPO). Value beyond the range clipped to supported min/max [**Default Max Frequency**, 100MHz, 150MHz, 200MHz ,.....1150MHz, 1200MHz]	
		Disable Turbo GT Frequency>	Enable or Disables the GT frequency, disable is not limited [Enabled, **Disabled**]	

Sub-screen	Next Level Sub-screens / Description			
PCH-FW Configuration>	Read Only field Firmware: version, mode, SKU, States 1, Status 2			
	ME State>	When disables ME goes into ME Temporarily Disabled Mode [**Enabled**, Disabled]		
	ME Unconfig. on RTC Clear>	When disables ME will not unconfigured on RTC clear [**Enabled**, Disabled]		
	Extended CSME Measured to TPM-PCR>	Read only field [Enabled, **Disabled**]		
	Core BIOS Done Message>	Enables or disable the core BIOS Done message sent to ME [**Enabled**, Disabled]		
	Firmware Update Configuration>	ME Firmware Image Re-flash>	Enables or disables the ME firmware image RE-flash function [Enabled, **Disabled**]	
		FW Update>	Enables or disables the ME firmware update function [**Enabled**, Disabled]	
		PTT Configuration>	TPM Device Selection>	Selects PTT, or dTPM] PTT enables PTT in SKuMgr dTPM 1.2 warning - Disabled PTT in SKuMgr Disables PTT/dTPM and all data saved on it will be lost. [dTPM, **PTT**]
		Anti-Rollback SVN Configuration>	Automatic Hardware Enforced Anti-rollback SW>	Anti-rollback automatically active once ME FW successfully runs on platform. Firmware with the lower ARB-SVN is blocked from execution [Enabled, **Disabled**]
			Set HW-enforced Anti-Rollback for Current SVN>	Hardware enforced anti-rollback for current ARB-SVN value. Firmware with lower ARB-SVN is blocked from execution. Value will be restored to disable after the command is sent. [Enabled, **Disabled**]

Sub-screen	Next Level Sub-screens / Description			
PCH-FW Configuration> (continued)	Firmware Update Configuration> (continued)	OEM Key Revocation Configuration>	Automatic OEM Key Revocation>	Enable: Bios automatically sends HECI command to revoke OEM keys. [Enabled, **Disabled**]
			Invoke OEM Key Revocation>	Enable: HECI command sent to revoke OEM key [Enabled, **Disabled**]
Sub-screen	Next Level Sub-screens / Description			
Thermal Consideration>	Enable all Thermal Functions>	Enable: for memory thermal management, active trip points, critical trip points. Disable: for manual configuration [**Enabled**, Disabled]		
	CPU Thermal Configuration>	DTS SMM>	Disable: uses ED reported temperature values. Enable: uses DTS SMM mechanism to obtain CPU temperature values. Out of Spec: uses EC reported temp values and DTS SMM and DTS is used to handle Out of Spec condition [Enabled, **Disabled,** Critical Temp Reporting]	
		TCC Active Offset>	TCC active Offset rage [0 to 63] Temperature at which the thermal control circuit must be activated. [**0**]	
		TCC Offset Time Window>	For Running Average Temperature Limits (RATL) feature, the offset time range is 5 ms to 448 s. [**Disabled**, 10ms, 55ms …… 192sec, 224sec, 254sec]	
		TCC Offset Clamp Enable>	For Running Average Temperature Limits (RATL) feature, to allow CPU to throttle below P1 [Enabled, **Disabled**]	
		TCC Offset Lock Enable>	For Running Average Temperature Limits (RATL) feature, to lock temperature target MSR. [**Enabled**, Disabled]	
		Bi-directional PROCHOT#>	When processor thermal sensor trips (either core) PROCHOT# will be driven. When bi-directional enabled external agents drive PROCHOT# to throttle the processor. [**Enabled**, Disabled]	
		Disable PROCHOT# Output>	[**Enabled**, Disabled]	
		Disable VR Thermal Alert>	[Enabled, **Disabled**]	
		PROCHOT Response>	[Enabled, **Disabled**]	
		PROHOT Lock>	[Enabled, **Disabled**]	
		ACPI T-States>	[Enabled, **Disabled**]	
	Platform Thermal Configuration>	Critical Trip Point>	Controls temperature of ACPI Critical Trip Point, at which OS shuts down the system. Note: 119 C is the PLAN of Record (POR) for all Intel mobile processors. [15 C , 23 C, 31 C……**119 C (POR)**, 127 C, 130 C]	

Sub-screen	Next Level Sub-screens / Description		
Thermal Consideration> (continued)	Platform Thermal Configuration> (continued)	Critical trip Points>	[**Enabled**, Disabled]
		PCH Temp Read>	[**Enabled**, Disabled]
		CPU Energy Read>	[**Enabled**, Disabled]
		CPU Temp Read>	[**Enabled**, Disabled]
		Alert Enable Lock>	Locks all Alert enable settings. [Enabled, **Disabled**]
		CPU Temp>	Fail safe temp that EC uses if OS hangs [**72**]
		CPU Fan Speed>	Fan speed EC uses is OS hangs [**65**]
Sub-screen	**Next Level Sub-screens / Description**		
Platform Settings>	HID Event Filter driver>	Enable or disable the HID event filter driver interface to OS [**Enabled**, Disabled]	
	System Time and Alarm Source>	Selects source of system time and alarm functions [**ACPI Time and Alarm Device**, Legacy RTC]	
	Intel® Trusted Device Setup Boot>	Enable or disable Intel® trusted setup boot on the next boot. [Enabled, **Disabled**]	
Sub-screen	**Next Level Sub-screens / Description**		
ACPI D3Cold Settings>	ACPI D3Cold Support>	[**Enabled**, Disabled]	
	VR Ramp up Delay>	Delay between subsequent VR ramp ups if they are all turned on at the same time [**16**]	
	PCIE Slot 5 Device Power-On-Delay in ms>	Delay between applying core power and deasserting PERST# [**100**]	
	Audio Delay>	Delay after applying power to HD Audio (REALtek) codec device. [**200**]	
	SensorHub>	Delay after applying power to sensor hub [**68**]	
	TouchPad>	Delay after applying power to touchpad device [**68**]	
	TouchPanel>	Delay after applying power to touch panel device [**68**]	
	P-State Capping>	Set _PPC and send ACPI notification [Enabled, **Disabled**]	
	USB Port 1>	USB RTD3 support for super speed USB 3.0 and high speed USB 2.0 devices [Enabled, **Disabled**]	
	USB Port 2>	USB RTD3 support for super speed USB 3.0 and high speed USB 2.0 devices [Enabled, **Disabled**]	
	ZPODD>	Zero power ODD (ZPODD) only for boar with SPODD support [Enabled, **Disabled**]	

Sub-screen	Next Level Sub-screens / Description		
ACPI D3Cold Settings> (continued)	WWAN>	Read only field [**D0/L1.2**]	
	SATA Port 0>	Control the SATA port RTD3 functionality [Enabled, **Disabled**]	
	SATA Port 1	Control the SATA port RTD3 functionality [**Enabled**, Disabled]	
	SATA Port 2>	Control the SATA port RTD3 functionality [Enabled, **Disabled**]	
	SATA Port 3>	Control the SATA port RTD3 functionality. [Enabled, **Disabled**]	
	SATA Port 4>	Control the SATA port RTD3 functionality. [Enabled, **Disabled**]	
	SATA Port 5>	Control the SATA port RTD3 functionality. [Enabled, **Disabled**]	
	PCIe Remapped CR1>	PCIe RTD3 setup conflicts with SATA RTD3. [Enabled, **Disabled**]	
	PCIe Remapped CR2>	PCIe RTD3 setup conflicts with SATA RTD3. [Enabled, **Disabled**]	
	PCIe Remapped CT3>	PCIe RTD3 setup conflicts with SATA RTD3. [Enabled, **Disabled**]	
Sub-screen	**Next Level Sub-screens / Description**		
PCIE Configuration>	IMR Configuration>	PCIe IMR>	[Enabled, **Disabled**]
Sub-screen	**Next Level Sub-screens / Description**		
Trusted Computing>	Read only field TPM 2.0 device, Firmware version, Vendor		
	Security Device Support>	BIOS support for security device. OS will not show security device. TCG EFI protocol and INT1A interface will not be available. [**Enabled**, Disabled]	
	Active PCR Banks>	Read Only Field [**SHA256**]	
	Available PCR Banks>	Read only field [**SHA-1, SHA256, SHA384, SM3**]	
	SHA-1 PCR Bank>	[Enabled, **Disabled**]	
	SHA-1 PCR Bank>	[**Enabled**, Disabled]	
	SHA256 PCR Bank>	[Enabled, **Disabled**]	
	SH3_256 PCR Bank>	[Enabled, **Disabled**]	
	Pending operation>	Schedule an operating for security device. Note: computer reboots during restart to change the state of security device. [**None**, Clear]	
	Platform Hierarchy>	[**Enabled**, Disabled]	

Sub-screen	Next Level Sub-screens / Description		
Trusted Computing> (continued)	Storage Hierarchy>	[**Enabled**, Disabled]	
	Endorsement Hierarchy>	[**Enabled**, Disabled]	
	TPM 2.0 UEFI Spec Version>	TCG_1_2: compatible mode for WIN8/WIN10 TCG_2: support for TCG2 protocol and event format for win 10 or later [TCG_1_2, **TCG_2**]	
	Physical presence Spec Version>	OS supports PPI Spec 1.2 or 1.3. Note: Some HCL tests might not support 1.3. [1.2, **1.3**]	
	TPM 2.0 Interface Type>	Read only field [**CRB**]	
	Device Select>	Supports TPM 1.2 only, TPM 2.0 Only or both with auto where TPM 2.0 is default and then TPM 1.2 if default not found. [TPM 1.2, TPM 2.0, **Auto**]	
Sub-screen	**Next Level Sub-screens / Description**		
ACPI Settings>	Enable ACPI Auto Configuration>	[Enabled, **Disabled**]	
	Enable 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>	Selects the highest ACPI sleep state the system will enter when suspend is pressed. [Suspend Disabled, **S3 (suspend to Ram)**]	
Sub-screen	**Next Level Sub-screens / Description**		
Miscellaneous>	Generic eSPI Decode Ranges>	Generic LPC via eSPI Decode 1>	[Enabled, **Disabled**]
	Watchdog>	Auto–Reload>	Automatic reload of watchdog timers on timeout [Enabled, **Disabled**]
		Global Lock>	Enable: watchdog registers (except WD-Kick) read only until board is reset- [Enabled, **Disabled**]
		Stage 1 Mode>	Selects action for this stage [**Disabled**, reset, Delay, WDT Signal only]
	Rest Button Behavior>	Selects reset button behavior [**Chipset Reset**, Power Cycle]	
	I2C Speed>	Speed in KHz (Min. 1 KHz and max. 400KHz. 200KHz is an appropriate default value. [**200**]	
	Onboard I2C Mode>	Selects Multi master or Busclear [**Multimaster**, Busclear]	
	Manufacture Mode>	Read only field [Enabled, **Disabled**]	
	Lid Switch Mode>	Shows or hides LID switch in ACPI OS. [Enabled, **Disabled**]	
	Sleep Button Mode>	Shows or hides sleep button in ACPI OS [Enabled, **Disabled**]	

Sub-screen	Next Level Sub-screens / Description	
Miscellaneous> (continued)	ACPI Temperature Polling>	Sets mode for temperature polling through OSPM (0: disabled, 1: enabled) [**Enabled**, Disabled]
	TZ00 Temperature Polling Time>	Interval (sec) between two temperature measuring attempts in ACPI thermal zone 00 (Ambient temperature) [**30]**
	Create ACPI AC adapter>	Creates ACPI AC adapter device with virtual battery even in non-battery systems. This help some device drivers to identify the power status of the system. [**Enabled**, Disabled]
	SMbus Device ACPI Mode>	SM bus device is hidden or visible in OS [Hidden, **Normal**]
	CPLD Device ACPI Mode>	CPLD device is hidden or visible in OS [Hidden, **Normal**]
	Control COMe GPIOs in BIOS>	GPIO control in BIOS- If disable GPIO are not touched by BIOS [Enabled, **Disabled**]
	GPIO IRQ#>	Sets IRQ# to trigger by the CPLD on GPIO event. [Enabled, **Disabled**]
	I2C IRQ#>	Sets the IRQ number to trigger by cPLD on I2C event. [Enabled, **Disabled**]
	Local FW Update>	Allows BIOS re-flashing if Relax Security Configuration is set as enabled. Only Valid for one reset cycle! [Enabled, **Disabled**]
	Last System Reset Through>	Read only field [**Other/Software**]
Sub-screen	**Next Level Sub-screens / Description**	
Smart settings>	Smart Self test>	Runs Smart self-test on all HDDs during Post [Enabled, **Disabled**]
Sub-screen	**Next Level Sub-screens / Description**	
Hardware Monitor>	Read only field H/W Monitor type, CPU temperature, and Modules temperature value	
	CPU Fan>	
	Fan Control>	Sets fan control mode where disable totally stops the fan. [Disabled, Manual**, Auto**]
	Fan Pulse>	No. Pulses the fan produces during one revolution (range 1 to 4) [**2**]
	Fan Trip Point Speed>	Temperature where the fan accelerates. (range 20 to 80 C) [**50**]
	Trip Point Speed>	Fan speed at trip point in % (30 Min. Fan always runs at 100% at TJMax 10 C.[**50**]
	Reference Temperature>	Determines the temperature source used for automatic fan control [**CPU temperature**, Module temperature]
	External Fan>	
	Fan Control>	Sets fan control mode where disable totally stops the fan. [Disabled, Manual**, Auto**]
	Fan Pulse>	No. Pulses the fan produces during one revolution (range 1 to 4) [**2**]

Sub-screen	Next Level Sub-screens / Description		
Hardware Monitor> (continued)	Fan Trip Point Speed>	Temperature at which the fan accelerates (range 20 to 80 C) [**50**]	
	Trip Point Speed>	Fan speed at trip point in % (30 Min.) Fan always runs at 100% at TJMax 10 C.[**50**]	
	Reference Temperature>	Determines the temperature source used for automatic fan control [CPU temperature, **Module temperature**]	
	5.0V Standby>	Read only field [**5.2 V**]	
	Menu Batt Volt at COMe Pin>	Read only field [**3.02 V**]	
	Wider Range VCC>	Read only field [**12.22 V**]	
Sub-screen	**Next Level Sub-screens / Description**		
UEFI Variables Protection>	Password Protection of Runtime Variables>	Controls NVRA; runtime variable protection through system admin Password. [**Enabled**, Disabled]	
Sub-screen	**Next Level Sub-screens / Description**		
Serial Port Consol Redirection>	COM0(PCI Bus0, Dev30, Func0, Port1)		
	Console Redirection>	[Enabled, **Disabled**]	
	Console redirection settings		
	COM1(PCI Bus0, Dev30, Func1, Port1) (disabled) Console Redirection — Port is disabled		
	COM2(PCI Bus0, Dev0, Func0) (disabled) Console Redirection — Port is disabled		
	Serial port for out of Band management/Windows emergency Management Services (EMD)		
	Console Redirection EMS>	[Enabled, **Disabled**]	
Sub-screen	**Next Level Sub-screens / Description**		
AMI Graphics Output Protocol Policy>	Read only field Intel® Graphics Controller / Intel® GOP Driver [18.0.1031]		
	Output Select>	Selects output Interface [**eDP1**, DVI1]	
	BIST Enable>	Starts of stops BIST on the integrated display panel [Enabled, **Disabled**]	
Sub-screen	**Next Level Sub-screens / Description**		
SIO Common Settings>	Lock legacy resource>	[Enabled, **Disabled**]	
Sub-screen	**Next Level Sub-screens / Description**		
SIO Configuration>	Active Serial port>	Use this Device	Enable or disable use of this logical device [**Enabled**, Disabled]
		Logical Device Settings Current>	Read only field IO=2F8h; IRQ=3;

Sub-screen	Next Level Sub-screens / Description		
SIO Configuration> (continued)	Active Serial port> (continued)	Possible: Use Automatic Settings>	Allows the user to change the device's resource settings. New settings are reflected on the setup page after system restart. [**Use Automatic Settings**, IO=3F8h; IRQ=4, DMA; IO=3F8h; IRQ=3,4,5,7,9,10,11,12; DMA; IO=2F8h; IRQ=3,4,5,7,9,10,11,12; DMA; IO=3E8h, DMA; IRQ=3,4,5,7,9,10,11,12; DMA; IO=2E8h; IRQ=3,4,5,7,9,10,11,12; DMA]
	Warning! Disabling SIO logical devices may have unwanted side effects. Proceed with caution!		
	Active Parallel Port>	Use this Device>	Enable or disable use of this logical device [**Enabled**, Disabled]
		Logical Device Settings Current>	Read only field IO=378h; IRQ=5;
		Possible: Use Automatic Settings:>	Allows the user to change the device's resource settings. New settings are reflected on the setup page after system restart. [**Use Automatic Settings**, IO=378h; IRQ=5, IO=378h; IRQ=5,6,7,9,10,11,12 IO=2F8h; IRQ=5,6,7,9,10,11,12, IO=3E8h, DMA; IRQ=5,6, 7,9,10,11,12 IO=2E8h; IRQ=5,6,7,9,10,11,12]
		Mode>	[**STD Printer Mode**, SPP Mode, EPP-1.9 and SPP mode, EPP-1.7 and SPP mode, ECP Mode, ECP and EPP 1.9 Mode, ECP and EPP 1.7 mode]
	Warning! Disabling SIO logical devices may have unwanted side effects. Proceed with caution!		
	Warning! Changes made during setup session will be shown after you restart		
Sub-screen	**Next Level Sub-screens / Description**		
PCI Sub System Settings>	PCI Settings Common for all Devices:		
	BME DMA Mitigation>	Re-enable Bus Master Attribution disabled during PCI enumeration for PCI Bridge after SMM locked. [Enabled, **Disabled**]	
	Change settings of the following PCI devices: Warnings: Changing the PCI device settings may have unwanted side effects. System may hang! Proceed with caution.		
Sub-screen	**Next Level Sub-screens / Description**		
USB Configuration>	Read only field USB module version Controller and devices		
	Legacy Support>	Auto: disable legacy if no USB devices are connected Disable: keeps USB devices available only for EFI applications [**Enabled**, Disabled, Auto]	
	XHCI Hand-off>	This is a work around for OSs without XHCI hand-off support. The XHCI ownership change should be claimed by XHCI driver [**Enabled**, Disabled]	
	USB Mass Storage Driver Support>	[**Enabled**, Disabled]	

Sub-screen	Next Level Sub-screens / Description		
USB Configuration> (continued)	USB hardware delays and timeouts:		
	USB Transfer Time-outs>	Time out value for control, Bulk and interrupt transfers. [**20 sec**]	
	Device Reset Timeout>	USB Mass Storage device start unit command timeout [**20 sec**]	
	Device Power-Up Delay>	Max time device takes before reporting properly to host controller Auto uses default value: 100 ms for a root port, for a Hub port the delay is taken from HUB descriptor. [**AUTO**]	
Sub-screen	**Next Level Sub-screens / Description**		
Network Stake Configurator>	Network Stack>	Enable or disable UEFI network stack. [Enabled, **Disabled**]	
Sub-screen	**Next Level Sub-screens / Description**		
NVMe>	Read only field No device found in the system		
Sub-screen	**Next Level Sub-screens / Description**		
SDIO Configuration>	SDIO Access Mode>	Auto: Access SD device in DMA mode if controller supports DMA mode, else in PIO Mode DMA: access SD device in DMA mode PIO: access SD in PIO mode [**Auto**, ADMA, SDMA, PIO]	
	Mass Storage Devices		
	eMMC S0J57X(31.8GB)>	Mass storage device emulation type. Auto: enumerates devices less than 530 MB as floppies. Forced FDD: forces HDD formatted drive to boot FDD [**Auto**, Floppy, Forced FDD, hard Disk]	
Sub-screen	**Next Level Sub-screens / Description**		
RAM Disk Configuration>	Disk Memory Type>	Specifies type of memory to use from the available memory pool in system to create a disk [**Boot Service Data**, Reserved]	
	Create RAW>	Size Hex>	Valid RAM disk size should be multiples of the RAM disk block size [**1**]
		Create & Exit>	Create a new RAM disk with the given starting and ending address
		Discard & Exit>	Discard and exit
	Create from File>	Create a RAM disk from a given file select available storage device. [**HDD SATA 96 MB**]	
	Remove Selected RAM Disk (s)>	Remove selected RAM disks	
Sub-screen	**Next Level Sub-screens / Description**		
User Password Management>	Admin Password Management>	Read only field [**Not Installed**]	
	Change Admin Password>	New password must be between 8 and 32 Characters include lower and upper case, number and symbol. Note: input old admin password I fit was set, then you can change the password to a new one. After the change action you may need to enter the password when you enter UI.	

6.4.3. Chipset Setup Menu

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

Figure 14: Chipset Setup Menu

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

Table 27: Chipset Setup Menu Sub-screens and Functions

Sub-screen	Next Level Sub-screens / Description				
Firmware Configuration>	Firmware Configuration option. Note Ignore policy update is to skip policy update and will only work on a platform. [Ignore Policy Update, Production, Test]				
Sub-screen	Next Level Sub-screens / Description				
System Agent (SA) Configuration>	VT-d >	Read only field Memory configuration parameters [**Supported**]			
	Memory Configuration>	Memory Thermal Configuration>	Memory Power and Thermal Throttling>	DDR Power Down and Idle Counter>	BIOS Controls DDR CKE mode and idle timer value. PCODE manages the mode [PCODE, **BIOS**]
				For LPDDR: DDR Power Down and Idle Counter>	BIOS controls DDR CKE mode and idle timer value. PCODE manages the mode [PCODE, **BIOS**]

Sub-screen	Next Level Sub-screens / Description				
System Agent (SA) Configuration> (continued)	Memory Configuration> (continued)	Memory Thermal Configuration> (continued)	Memory Power and Thermal Throttling> (continued)	Refresh_2X_ Mode>	[Disables, **1- Enabled for Warm or Hot**, 2- Enabled Hot only]
				LPDDR Thermal Sensor>	When enables MC uses MR4 to read LPDDR thermal sensors [**Enabled**, Disabled]
				Self Refresh Enable>	[**Enabled**, Disabled]
			Memory Thermal Management>	[Enabled, **Disabled**]	
		Read only field Memory configuration: RC Version, Date rate and Timings. Slot information (populate (size, rank, manufacturer), not populated) Memory ratio and clocking/overclocking			
		MCR ULT Safe Config.>	MCR ULT safe Configuration for P0 [Enabled, **Disabled**]		
		Safe Mode Support>	Used for changes that may affect a stable MRC [Enabled, **Disabled**]		
		Maximum Memory Frequency>	Maximum frequency (MHz) must divide by 133 or 100 according to RefCLK. In GEAR2 must divide by 2666 or 200. Lowest GEAR2 speed is 2133. [**Auto**, 1067, 1200….. 4200, 4267		
		Max TOULD>	Dynamic assignment adjusts TOLUD automatically based on the largest MMIO length [**Dynamic**, 1GB, 1,25 GB, 1.5 GB ….. 3.35 GB, 3.5 GB]		
		SA GV>	System Agent Geyserville enables/disables frequency switching or fix to a specific point. [Disable, Fixed Low, Fixed Mid, Fixed High, **Enabled**]		
		Enables RH Prevention>	Actively prevent row hammer [**Enabled**, Disabled]		
		Row Hammer Solution>	Method to prevent row hammer [**2x refresh**]		
		Power Down Mode>	CKE power Down Mode Control [**Auto**, No Power Down, APD, PPD-DLLoff]		
		Memory Scrambler>	Enables/ disable memory scrambler support [**Enabled**, Disabled]		
		Force ColdReset>	Force Coldreset or Choose MrcColdBoot mode, when Coldboot is required during MRC execution- If ME 5 MB, Force Coldreset is required! [Enabled, **Disabled**]		
		Memory Remap>	Memory remap above 4 GB [**Enabled**, Disabled]		
		Fast Boot>	Fast path through the MRC [**Enabled**, Disabled]		

Sub-screen	Next Level Sub-screens / Description			
System Agent (SA) Configuration> (continued)	Memory Configuration> (continued)	Train On Warm Boot>	[Enabled, **Disabled**]	
		BDAT Memory Test Type>	Read Only field [**Rank margin Tool Rank**]	
	Graphics Configuration>	Skip Scanning of Exernal Gfx Card>	Enabled- will not scan for external Gfx card on PEG and PCH PCIe ports [Enabled, **Disabled**]	
		Primary Display>	Select the graphics device which is the primary display or select HG for hybrid Gfx. [**Auto**, IGFX, PEG, PCI]	
		External Graphics Cards Primary Display Configuration>	Primary PCI>	Select: Auto/PCIE1 to PCIe7 of D28: F0 to F7, PCIE8 to PCIE15 of D29: F0 to FF7, PCIE16 to PCIe19 of D27: F0 to F3, Graphics device should be primary PCIE [**Auto**, PCIE1, PCIe2, …….. PCIE18, PCIE19]
		Internal Graphics>	[**Auto**, Disabled, Enabled]	
		GTT Size>	[2MB, 4MB, **8MB**]	
		Aperture Size>	[128MB, **256MB**, 512MB, 1024MB, 2048MB]	
		DVMT Pre-allocated>	Selects the pre-allocated (fixed) graphics memory size used by the internal device [32M, 64M, 96M 128M, 160M, 4M, 8M, 12M , 16M, 20M, 24M, 28M, 32M/F7, 36M, 40M, 44M, 48M, 52M, 56M , **60M**]	
		DVMT Total Gfx Mem>	Selects the total graphics memory size used by the internal device [128M, **256M**, Max]	
		PM Support>	[**Enabled**, Disabled]	
		PAVP Enable>	[**Enabled**, Disabled]	
	VT-d>	[**Enabled**, Disabled]		
	X2APCI Opt Out>	[**Enabled**, Disabled]		
	DMA Control Guarantee>	[Enabled, **Disabled**]		
	IGD VTD Enable>	[**Enabled**, Disabled]		
	IPU VTD Enable>	[Enabled, **Disabled**]		
	IOP-VTD Enable>	[**Enabled**, Disabled]		
	ITBT VTD Enable>	[Enabled, **Disabled**]		
	CPU Crash Log (Device 10)>	[Enabled, **Disabled**]		

Sub-screen	Next Level Sub-screens / Description			
System Agent (SA) Configuration> (continued)	CRID Support>	SA CRID and TCSS CRID control for Intel SIPP [Enabled, **Disabled**]		
	Above 4 GB MMIO BIOS Assignment>	Enables automatically when aperture size is set to 2048 MB. [**Enabled**, Disabled]		
Sub-screen	**Next level Sub-Screens / Description**			
PCH-IO Configuration>	PCI Express Configuration>	DMI Link ASPM Control>	Control of Active State power management of the DMI [Disable, L0s, L1, L0sL1, **Auto**]	
		Peer Memory Write Enable>	[Enabled, **Disabled**]	
		Compliance Test Mode>	[Enabled, **Disabled**]	
		PCH PCI Express Clock Gating>	PCH PCI express clock gating (power management) for each root port. [Platform-POR, Enabled, **Disabled**]	
		PCIe Function Swap>	Disabled prevents PCIe root port function swap. If any function other than 0th is enabled, 0th will become visible. [**Enabled**, Disabled]	
		PCIe EQ Settings>	PCIe EQ Override>	Choose PCIe EQ setting. Only use when you have a thorough understanding of the equalization process. [Enabled, **Disabled**]
		PCIE Express Root Port [1 to 4]>	PCIe Express Root Port [#]>	Control the PCIe Express Root Port [**Enabled**, Disabled]
			Connection Type>	Built-in: A built-in device is connected to this root port. Slot implemented bit will be clear. Slot: This root port connects to a user accessible slot. Slot implemented boot will be set. [Built-in, **Slot**]
			ASPM>	Sets ASPM level: Force LO: Forces all links to L0 state Auto : BIOS auto configure Disable: Disables ASPM [Disable, L0s, L1, L0sL1, **Auto**]
			L1 Sub-states>	PCIe L1 sub-state settings: [**Disabled**, l1.1, l1.1 &L1.2]
			ACS>	Access Control Service [**Enabled**, Disabled]
			PTM>	Precision Time Measurement Enabled, **Disabled**]
			DPC>	Downstream Port Containment [**Enabled**, Disabled]

Sub-screen	Next Level Sub-screens / Description			
PCH-IO Configuration> (continued)	PCI Express Configuration> (continued)	PCIE Express Root Port [1 to 4]> (continued)	EDPC>	Extensions for Downstream Port Containment [**Enabled**, Disabled]
			URR>	Unsupported Request Reporting [Enabled, **Disabled**]
			FER>	Fatal error reporting [Enabled, **Disabled**]
			NFER>	Non- Fatal error reporting [Enabled, **Disabled**]
			CER>	Correctable error reporting [Enabled, **Disabled**]
			SEFE>	System error on fatal error [Enabled**, Disabled**]
			SENFE>	System error on non-fatal error [Enabled, **Disabled**]
			SECE>	System error on correctable error [Enabled, **Disabled**]
			PME SCI>	[**Enabled**, Disabled]
			Hot Plug>	[Enabled, **Disabled**]
			Advance Error Reporting>	[**Enabled**, Disabled]
			PCIE Speed>	Configure PCIe Speed [**Auto**, Gen1, Gen2, Gen3]
			Transmitter Half Swing>	[Enabled, **Disabled**]
			Detect Timeout>	Time (msec) the reference code waits for link to exit detect state for enabling ports before assuming no device and potentially disabling the port. [**0**]
			Extra Bus Reserved>	Extra bus reserved (0-7) for bridges behind this root bridge **0**]
			Reserved Memory>	Range (1-20 MB) for this root port. [1**0**]
			Reserved I/O>	Reserved IO Range (4K, 8K, 12K, 16K, 20K) for this port. [**4**]
			PCH PCIe LTR Configuration	
			LTR>	PCIe latency reporting [**Enabled**, Disabled]
			Snoop Latency Override>	Disabled- disable override Manual- Manually enter override values Auto- maintain default BIOS flow [Disabled, Manual**, Auto**]

Sub-screen	Next Level Sub-screens / Description				
PCH-IO Configuration> (continued)	PCI Express Configuration> (continued)	PCIE Express Root Port [1 to 4]> (continued)	Non Snoop Latency Override>	Disabled- disable override Manual- Manually enter override values Auto- maintain default BIOS flow [Disabled, Manual, **Auto**]	
			Force LTR Override>	Enabled: LTR override values forced and LTR messages from the device ignored Disabled: LTR override values are not forced [Enabled, **Disabled**]	
			LTR Lock>	PCIe LTR configuration lock [Enabled, **Disabled**]	
			Extra Options>	Detect Non-Compliance Device>	When enable will take more post time [Enabled, **Disabled**]
				Prefetch Memory>	Prefetchable memory range for this root bridge [1**0**]
				Reserved Memory Alignment>	Range (0 to 31 bits) [**1**]
				Prefetchable Memory Alignment>	Range (0 to 31 bits) [**1**]
		PCI Clock>	Clock0 Assignment>	Platform-POR: clock assigned to PCIe port or LAN according to module layout Enable- keep clock even if unused Disable- disable clock [Platform-POR, **Enabled**, Disabled]	
			ClkReq for Clock0>	Platform-POR: CLKREQ signal assigned to CLKSRC according to module layout Disable- disable clock [Platform-POR, **Disabled**]	

Sub-screen	Next Level Sub-screens / Description			
PCH-IO Configuration>	SATA Configuration>	SATA Controllers>	[**Enabled,** Disabled]	
		SATA Port Multiplier>	Determines how the SATA controllers(s) operate [**AHCI**]	
		SATA Mode Selection>	[Enabled, **Disabled**]	
		SATA Test Mode>	[Enabled, **Disabled**]	
		Software Feature Mask Configuration>	HDD Unlock>	Enabled: Indicates HDD password unlock in OS is enabled [**Enabled,** Disabled]
			LED Locate>	Enabled: Indicates LED/SGPIO hardware is attached and ping to locate feature is enabled on OS [**Enabled,** Disabled]

Sub-screen	Next Level Sub-screens / Description		
PCH-IO Configuration>	SATA Configuration> (continued)	Aggressive LPM Support>	Enable PCH to aggressively enter link power state [Enabled, **Disabled**]
		Serial ATA>	Read only field **CT120BX500SSD1 (120.0 GB)**
		Software Preserve>	Read only Field **SUPPORTED**
		Port [#]>	Enable or disable the SATA port [0 or 1] [**Enabled**, Disabled]
		Hot Plug>	Designates port as hot pluggable [Enabled, **Disabled**]
		Configure as eSATA>	Read only Field **Hot Plug Supported**
		External>	Marks port as External [Enabled, **Disabled**]
		SPIN Up Device>	Enable staggered spin up performed only on drives with option enabled spin up at boot. Otherwise all drives spin up at boot [Enabled, **Disabled**]
		SATA Device Type>	Identified the drive type [**Hard Disk Drive**, Solid State drive]
		Topology>	Identify the SATA topology [**Unknown**, SATA, Direct Connect, Flex, M2]
		SATA Port 0 DevSLP>	For DevSLP both hard drive and SATA port need to support DevSLP function otherwise, unexpected behavior might happen. Check module design before enabling. [Enabled, **Disabled**]
		SATA Port 0 RXPolarity>	Disable is default- check module design before enabling. [Enabled, **Disabled**]
		DITO Configuration>	[Enabled, **Disabled**]
		DITO Value>	Read Only port [**625**]
		DM value>	Read Only port [**15**]
Sub-screen	**Next Level Sub-screens / Description**		
PCH-IO Configuration>	USB Configuration>	XHCI Compliance Mode>	Disabled is default Change to enable for Compliance mode testing [Enabled, **Disabled**]
		XDCI Support>	Read only field [Enabled, **Disabled**]
		USB2 PHY Sus Well Power Gating>	Enable Sus well PG for USB2 PHT. Has no effect on PCH-H. [**Enabled**, Disabled]

Sub-screen	Next Level Sub-screens / Description			
PCH-IO Configuration> (continued)	USB Configuration> (continued)	USB3 Link Speed Selection>	Selects USB3 link speed [**GEN 1**, GEN2]	
		USB PDO Programming>	Select if port Disable Override (PDO) used [**Enabled**, Disabled]	
		USB Overcurrent>	Disable for pin-based debug. If Pin-based debug enabled and USB overcurrent is not disabled, USB Dbc does not work. [**Enabled**, Disabled]	
		USB Over Current Lock>	Select if USB Over current used. Enabling make xHC controller consume Overcurrent mapping data [**Enabled**, Disabled]	
		USB port Disable Override>	Enable or disable the corresponding USB port from reporting a device connection to the controller [**Disabled**, select per-Pin]]	
		USB Device/HOST Mode Override>	Enable or disable the corresponding USB 2.0 and USB 3.0 port device mode [**Disabled**, select per-Pin]	
Sub-screen	**Next Level Sub-screens / Description**			
PCH-IO Configuration>	Security Configuration>	RTC Memory Lock>	Enable Locks bytes 38h-3Fh in the lower/upper 128-byte bank of RTC RAM [**Enabled,** Disabled]	
		BIOS Lock>	PCH BIOS Lock enable feature. Enable to ensure SMM protection of Flash. [**Enabled,** Disabled]	
Sub-screen	**Next Level Sub-screens / Description**			
PCH-IO Configuration>	HD Audio Configuration>	HD Audio>	Controls detection of the audio device Disable: HDA unconditionally disabled Enabled: HDA unconditionally enabled [**Enabled,** Disabled]	
		Audio DSP>	Enables or disables the Audio DSP. [Enabled, **Disabled**]	
		HD Audio Advanced Configuration>	iDisplay Audio Disconnect>	Disconnects the SDI2 signal to hide/disable iDisplay audio Codec [Enabled, **Disabled**]
			Codec Sx Wake Capability>	Capability to detect wake initiated by a codec in Sx (e.g. Modem codec) [Enabled, **Disabled**]
			PME Enable>	Enables PME wake of HD audio controller during post [Enabled, **Disabled**]
			Statically Switchable VBCLK Clock Frequency Config.	
			HD Audio Link Frequency>	Applicable only if HAD codec supports selected frequency [6 MHz, 12 MHz, **24 MHz**]

Sub-screen	Next Level Sub-screens / Description			
PCH-IO Configuration> (continued)	HD Audio Configuration> (continued)	HD Audio Advanced Configuration> (continued)	iDisplay Audio Link Frequency>	Selects iDisplay Link frequency [48 MHz, **96 MHz**]
			iDisplay Audio Link T-Mode>	Indicates whether SDI is operating in 1T, 2T (CNL) or 2T, 4T, 8T mode (ICL) [2T Mode, 4T mode, **8T Mode**, 16T Mode]
Sub-screen	**Next Level Sub-Screens / Description**			
PCH/IO Configuration>	Serial IO Configuration>	UART1 Controller (COMe UART0>	If device is function 0, PSF disabling is skipped. PSF default remains and device PCI CFG space will be visible. This is needed to allow PCI enumerator access functions above 0 in a multifunction device. The following devices depend on each other: I2C0 and I2C1,2,3 UART0 and UART1, SPIO, 1 UART2 and I2C,5 UART 0 (00:30:00) cannot be disabled when: Child device is enabled like CNVi Bluetooth (_SB.PC00.UA00.BTH0) UART 0 (00:30:00) cannot be enabled when: I2S Audio codec is enabled [Disabled, enabled, **Communication port (COM)**]	
		UART2 Controller (COMe UART1>	Set UART2 mode -DBG used for BIOS log print and/or Kernel OS debug -COM-16550 Compatibility serial power with power gating support [Disabled, enabled, **Communication port (COM)**]	
		Serial IO UART1 Settings>	Hardware Flow Control>	Enable: configures two additional GPIO pads for use as RTS/CTS signals for UART [Enabled, **Disabled**]
			DMA Enable>	Enable: UART OS driver uses DMA when possible Disable: OS driver enforces PIO mode [**Enabled**, Disabled]
		Serial IO UART2 Settings>	Hardware Flow Control>	Enable: configures two additional GPIO pads for use as RTS/CTS signals for UART [Enabled, **Disabled**]
			DMA Enable>	Enable: UART OS driver uses DMA when possibleDisable: OS driver enforces PIO mode [**Enabled**, Disabled]
Sub-screen	**Next Level Sub-Screens / Description**			
PCH/IO Configuration>	SCS Configuration>	eMMC 5.1 Controller>	[**Enabled,** Disabled]	
		eMMC 5.1 HS400 Mode>	[**Enabled,** Disabled]	

Sub-screen	Next Level Sub-screens / Description		
PCH/IO Configuration> (continued)	SCS Configuration> (continued)	Enable HS400 Software Tuning>	Software tuning should improve eMMC HS400 stability at the expense of boot time. [Enabled, **Disabled**]
		Driver strength>	Sets I/O driver strength [33 Ohm, **40 Ohm**, 50 Ohm]
		SD Card 3.0 Controller>	[Enabled, **Disabled**]
Sub-screen	**Next Level Sub-screens / Description**		
PCH/IO Configuration>	TSN GBE Configuration>	PSE TSN GBE 0 Multi-VC>	Enable or disable TSN Multi Virtual Channels. TSN GBE must be host owned. [Enabled, **Disabled**]
		PSE TSN GBE 0 SGMII Support>	Enable or disable Modphy support for SGMII mode with the same PLL common lane must use the same link speed. UFS needs to be disables as this post uses the same PLL common lanes. Make sure IFWI has the proper straps set for SGMII. Make sure FLEX IO lane assignment is not NONE. [**Enabled,** Disabled]
		PSE TSN GBE 0 Link Speed>	PSE TSN GBE 0 link speed configuration. [RefClk 38.4MHz 2.5Gbps, **RefClk 38.4MHz 1Gbps**]
		Flex IO Lane Assignment>	Read only field [**Lane 7**]
Sub-screen	**Next Level Sub-screens / Description**		
PCH/IO Configuration>	PCH Master Clock Gating Control>	[Disabled, **Default**]	
	PCH Master Power Gating Control>	[**Disabled**, Default]	
	State After G3>	State to go to when power is re-applied after a power failure (G3 State) [**S0 state**, S5 State]	
	Port 80h Redirection>	[**LPC Bus**, PCIE Bus]	
	Enhance Port 80h LPC Decoding>	Support the word/dwor decoding of port 80h behind LPC [**Enabled,** Disabled]	
	Legacy IO Low Latency>	Set the enable low latency of legacy OP. Some systems require lower Io latency irrespective of power. This is a tradeoff between power and IO latency. [Enabled, **Disabled**]	
	PCH Energy Reporting>	Enable energy Report. MUST set as ENABLED. This is only for test purposes. [**Enabled,** Disabled]	
	LPM S0i2.0>	Enables or disables the S0ix sub-states. This setting is for test purpose. S0ix sub-states should be enables for production. [**Enabled,** Disabled]	
	LPM S0i2.1>		
	LPM S0i2.2>		

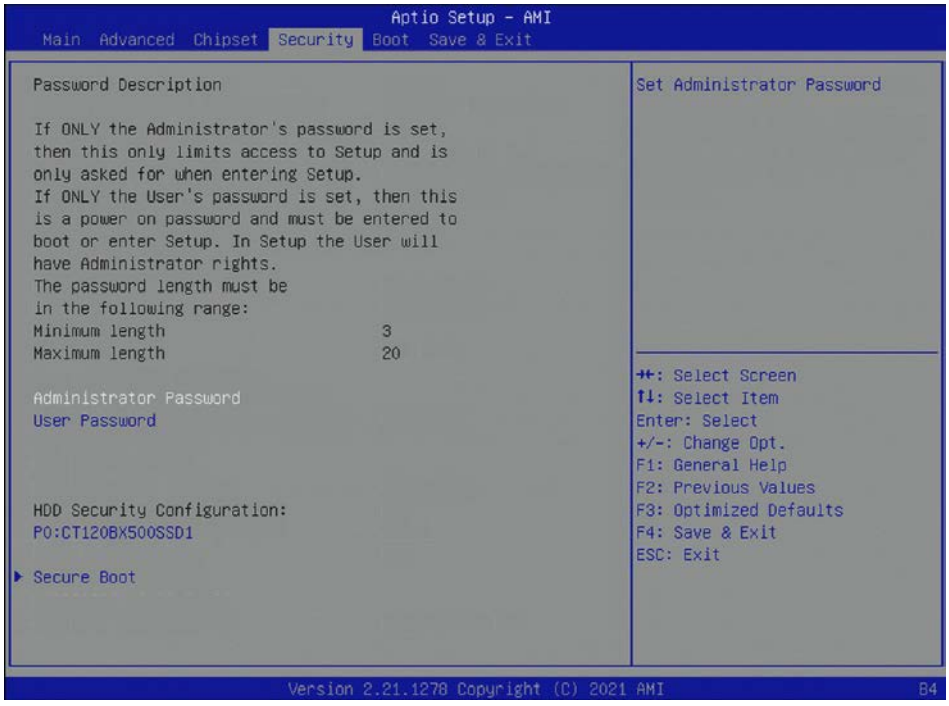
Sub-screen	Next Level Sub-screens / Description	
PCH/IO Configuration> (continued)	LPM S0i3.0>	
	LPM S0i3.1>	
	LPM S0i3.2>	
	LPM S0i3.3>	
	LPM S0i3.4>	
	IEH Mode>	Enable or Bypass IEH Mode [**Bypass**, Enabled]
	Enable TCO Timer>	When disables, it disables PCH ACPI timer, stops TCO timer abs ACPI WDAT table will not be published. [Enabled, **Disabled**]
	PCIe PLL SSC>	PCIe PLL SSC percentage Auto: Keep HW default, no BIOS override (range 0.0% to 2.0%) [**Auto**, 0.9%, 0.1%, 0.2%, …. 2.0%, Disabled]
	Flash Protection Range Register>	Enables the flash protection range registers (FRPP) [Enabled, **Disabled**]
	LGMR>	64 KB memory block for LGMR (LPC Memory Range Decode) [**Enabled,** Disabled]
	Extended BIOS Range Decode>	Enable: redirects memory cycles falling in a specific area to SPI flash controller. [Enabled, **Disabled**]
Sub-Screen	**Next level Sub-screens / Description**	
IGD Configuration>	Data Format>	Read only field [**EDID 1.4**]
	Resolution>	Read only field [**1024x768**]
	Color Depth>	Read only field [**24 bit**]
	Channel Count>	Read only field [**Single Channel**]
	eDP Port Configuration	
	eDP Port>	[**Enabled,** Disabled]
	Integrated eDP to LVDS Bridge>	[Disabled, **Auto**]
	LFP Resolution>	Selects the LFP used by internal graphics device: [**Auto,** Custom, PAID, VGA 640x480 1x18 WVGA 800x480 1x18, SVGA 800x600 1x18 XGA 1024x768 1x18, XGA 1024x768 1x24 WXGA 1280x768 1x24, WXGA 1280x800 1x18 WVGA 1366x768 1x24, WSVGA 1280x600 1x18 WSVGA 1280x600 1x24]
	Backlight Control>	Backlight control setting. [None/External, **PWM**, PWM Inverted, I2C, I2C Inverted]

Sub-screen	Next Level Sub-screens / Description	
IGD Configuration> (continued)	PWM Frequency>	Set LCD backlight PWM frequency. [**200 Hz**, 400 Hz, 1 kHz, 2 kHz, 4 kHz, 8 kHz, 20 kHz, 40 kHz]
	Backlight Value>	Set LCD Backlight brightness (1-255). [**255**]
	LVDS Clock Center Spreading>	Select the LVDS Clock frequency center spreading depth [**No Spreading**, 0.5%, 1.0%, 1.5%, 2.0%, 2.5%]

6.4.4. Security Menu

The security Setup menu lists sub-screens and second level sub-screens of the functions supported within the Security setup menu.

Figure 15: Security Setup Menu



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

Table 28: Security Setup Menu Sub-screens and Functions

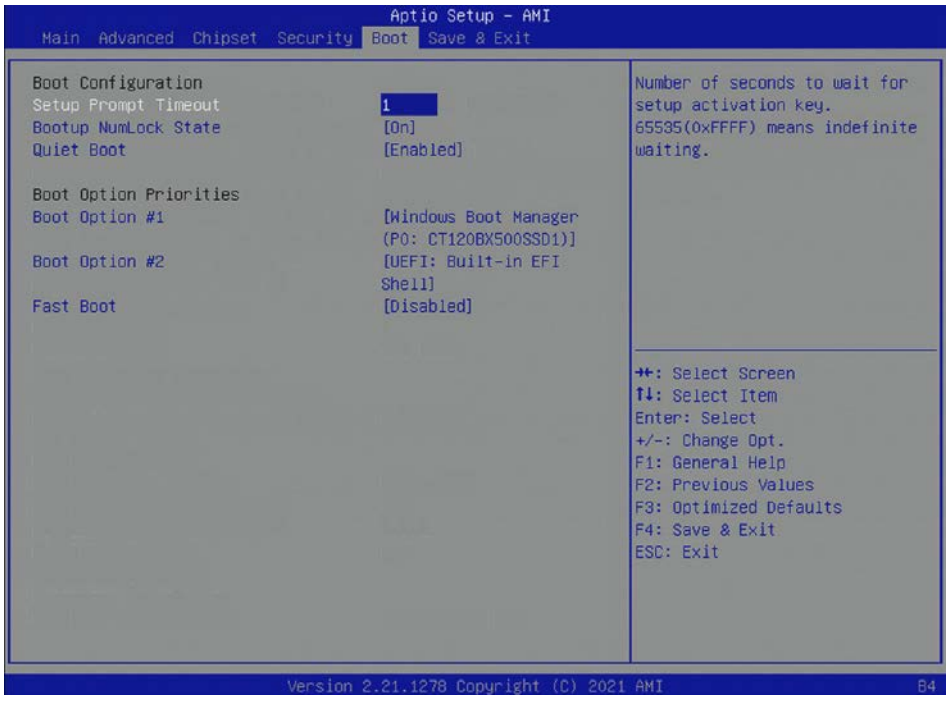
Sub-screen	Next Level Sub-screens / Description
Setup Administrator Password>	Sets administrator password
User Password>	Sets user password
HDD Security Configuration:	
P0: CT120BX500SSD1>	HDD Password description Allows access to set, modify and clear Hard Disk User Password. User Password mandatory to enable HDD Security If the 'Set user Password' is hidden, do power cycle to enable the option again. HDD Password Configuration: Security supported : Yes Security Enabled : No Security Locked : No Security Frozen : No HDD User Pwd Status : Not Installed HDD Master Pwd Status : Installed

Sub-screen	Next Level Sub-screens / Description		
P0: CT120BX500SSD1> (continued)	Set User Password>	Set HDD user password. Advisable to power cycle system after setting Hard Disk Passwords. Discard or save changes option in setup does not have any impact on HDD when password is set or removed. If the 'Set HDD User Password' option is hidden, power cycle to enable the option. again.	
Secure Boot>	Secure Boot>	Enable to activate. Platform key (PK) is enrolled and the system is in user mode. Mode change requires platform reset. [Enabled, **Disabled**]	
	Secure Boot Mode>	Custom: secure boot policy variable can be configured by a physically present user without full authentication. [Standard, **Custom**]	
	Restore Factor Keys>	Install factor defaults [Yes, No]	
	Reset to Set Up Mode>		
	Key Management>	Factory Key Provision>	Restore factory default after platform rest and while system is in setup mode [Enabled, **Disabled**]
		Restore Factor Keys>	Restore factor defaults [Yes, No]
		Reset to Set Up Mode>	
		Export Secure Boot Variables>	
		Enroll Efi Image>	Allows image to run in secure boot mode. Enroll SHA256 Hash certificate of a PE image into authorized signature Database (db). Select a file system from the available options.
		Device Guard Ready	
		Remove UEFI CA from DB>	
		Restore DB Defaults>	Restore DB variable to factor defaults [Yes, No]
		Secure Boot Variable	/ Size / Keys / Key source
		Platform Key>	Enroll factory defaults or load certificate from a file: 1. Public key certificate: a. EFI_Signature_List b. EFI_cert_X509 (DER) c. EFI_CERT_RSA2048 (bin) d. EFI_CERT_SHAXXX 2. Authenticated UEFI variable 3. EFI PE/COFF Image(SHA256) Key Source: Factory, External, Mixed
		Key Exchange Keys>	
		Authentication Signature>	
		Forbidden Signatures>	
		Authorize Timestamps>	
		OSRecovery Signatures >	

6.4.5. Boot Setup Menu

The Boot Setup menu lists sub-screens of the functions supported within the Boot setup menu.

Figure 16: Boot Setup Menu



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

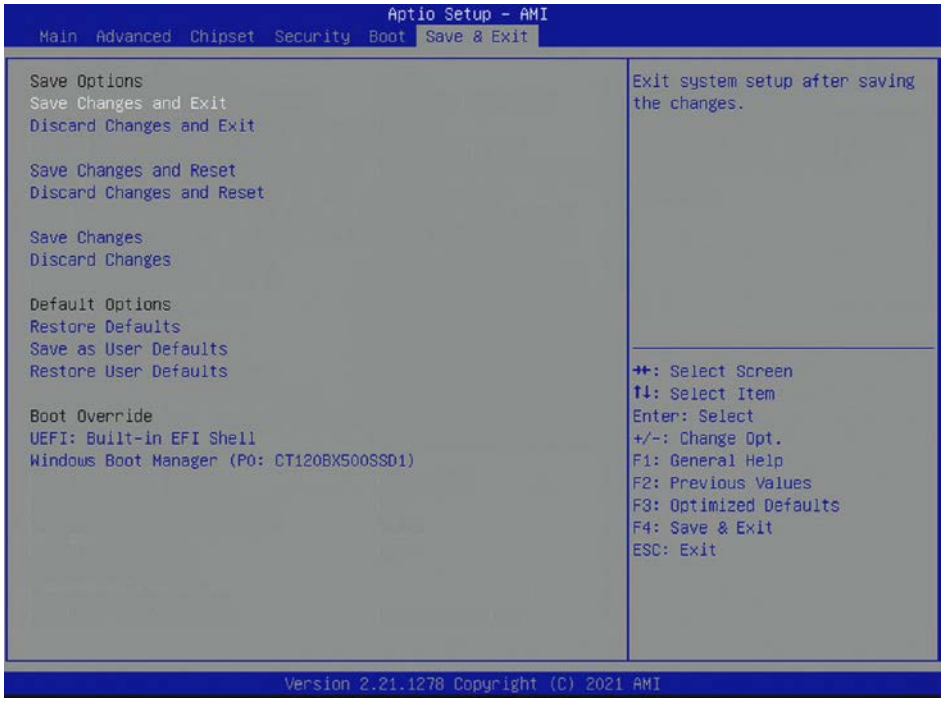
Table 29: Boot Setup Menu Sub-screens and Functions

Sub-screen	Description
Setup Prompt Timeout>	Number of seconds that the firmware waits for setup activation key The value 65535(0xFFFF) means an indefinite wait. [**1**]
Bootup NumLock State>	Selects keyboard NumLock state. [**ON**, OFF]
Quiet Boot>	Quiet Boot [**Enabled**, Disabled]
Boot Option Priorities:	
Boot Option #1>	Sets the system boot order [UEFI: Built in EFI Shell, **Windows Boot manager (P0 : CT120BX500SSD1)**, Disabled]
Boot Option #2>	Sets the system boot order [**UEFI: Built in EFI Shell**, Windows Boot Manager (P0 : CT120BX500SSD1), Disabled]
Fast Boot>	Enables or disables Boot with initialization of a minimal set of devices required to launch active boot option. Has no effect for BBS Boot option. [Enabled, **Disabled**]

6.4.6. Save and Exit Setup Menu

The Save and Exit Setup menu lists sub-screens of the functions supported within the Save and Exit setup menu.

Figure 17: Save and Exit Setup Menu



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

Table 30: Save and Exit Setup Menu Sub-screens and Functions

Sub-screen	Description
Save Options:	
Save Changes and Exit >	Exits system set up after saving changes [Yes, No]
Discard Changes and Exit>	Exits system setup without saving changes [Yes, No]
Save Changes and Reset>	Resets system after saving changes [Yes, No]
Discard Changes and Reset>	Resets system setup without saving changes [Yes, No]
Save Changes>	Saves changes made so far for any setup options [Yes, No]
Discard Changes>	Discards changes made so far for any setup options [Yes, No]
Default Options:	
Restore Defaults>	Restores/loads standard default values for all setup options [Yes, No]
Save as User Defaults>	Saves changes done so far as user defaults [Yes, No]
Restore User Defaults>	Restores user defaults to all setup options [Yes, No]
Boot Override:	
UEFI: Built in EFI Shell>	[Yes, No]
Windows Boot Manager (PO: CT120BX500SSD!9>	[Yes, No]

6.5. The uEFI Shell

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

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.
2. Press the <F7> key (instead of <DEL>) to display a choice of boot devices.
3. 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)
```

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

```
Shell>
```

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 relevant product information available:

- 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

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

Product ID, Serial Number and Revision are located on the module's bottom side.

7.1. Returning Defective Merchandise

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

1. Visit the RMA Information website:

   http://www.kontron.com/support-and-services/support/rma-information

2. Download the RMA Request sheet for **Kontron Europe GmbH- Deggendorf** 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.

8/ Warranty

Kontron defines product warranty in accordance with regional warranty definitions. Claims are at Kontron's discretion and limited to the defect being of a material nature. To find out more about the warranty conditions and the defined warranty period for your region, follow the steps below:

1. Visit Kontron's Term and Conditions webpage.

   http://www.kontron.com/terms-and-conditions

2. Click on your region's General Terms and Conditions of Sale.

8.1. Limitation/Exemption from Warranty Obligation

In general, Kontron shall not be required to honor the warranty, even during the warranty period, and shall be exempted from the statutory accident liability obligations in the event of damage caused to the product due to failure to observe the following:

- Safety instructions within this user guide
- Warning Instructions within this user guide
- Information and hints within this user guide

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.

List of Acronyms

Table 31: List of Acronyms

API	Application Programming Interface
BIOS	Basic Input Output System
BMC	Base Management Controller
bps	bits per second
BSP	Board Support Package
CAN	Controller Area Network
Carrier Board	Application specific circuit board that accepts a COM Express ® module
COM	Computer-on-Module
COMe-b	COM Express® b=basic 125 mm x 95 mm module form factor
COMe-c	COM Express® c=compact 95 mm x 95 mm module form factor
COMe-m	COM Express® m=mini 84 mm x 55 mm module form factor
DDC	Display Data Control
DDI	Digital Display Interface –
DDIO	Digital Display Input/Output
DIMM	Dual In-line Memory Module
DP	DisplayPort (digital display interface standard)
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
FRU	Field Replaceable Unit
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
IC	Integrated Circuit
I^2C	Inter integrated Circuit Communications
IOT	Internet of Things
ISA	Industry Standard Architecture
JILI	JUMPtec Intelligent LVDS Interface
KCS	Keyboard Controller Style
KVM	Keyboard Video Mouse
LAN	Local Area Network
LPC	Low Pin-Count Interface:
LPDDR	Low Power Double Data Rate
LPT	Line Printing Terminal
LSB	Least Significant Bit
LVDS	Low Voltage Differential Signaling
M.A.R.S.	Mobile Application for Rechargeable Systems
MCP	Multi-Chip Package
MEI	Management Engine Interface
MLC	Multi Level Cell
MTBF	Mean Time Before Failure
NA	Not Available
NC	Not Connected
NCSI	Network Communications Services Interface
NTC	Negative Temperature Coefficient
OPI	On Package Interface
OS	Operating System
PCH	PLatform Controller Hub
PCI	Peripheral Component Interface
PCIe	PCI-Express
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.
PSE	Programmable Service Engine

pSLC	pseudo Single Level Cell
PSU	Power Supply Unit
RoHS	Restriction of the use of certain Hazardous Substances
RTC	Real Time Clock
SAS	Serial Attached SCSI – high speed serial version of SCSI
SATA	Serial AT Attachment:
SCSI	Small Computer System Interface
SEL	System Event Log
SFX	Small Formfactor ATX
SGMII	Serial Gigabit Media Independent Interface
SLC	Single Level Cell
SMB	System Management Bus
SoC	System on a Chip
SOIC	Small Outline Integrated Circuit
SOL	Serial Over LAN

SPD	Serial Presence Detect
SPI	Serial Peripheral Interface
TCC	Time Coordinate Computing
TSN	Time Sensitive Networking
TPM	Trusted Platform Module
UART	Universal Asynchronous Receiver Transmitter
UEFI	Unified Extensible Firmware Interface
UFS	Universal Flash Storage
UHD	Ultra High Definition
USB	Universal Serial Bus
VGA	Video Graphics Adapter
VLP	Very Low Profile
WDT	Watch Dog Timer
WEEE	Waste Electrical and Electronic Equipement (directive)
WOL	Wake On LAN

About Kontron

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

Global Headquarters

Kontron Europe GmbH

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

www.kontron.com