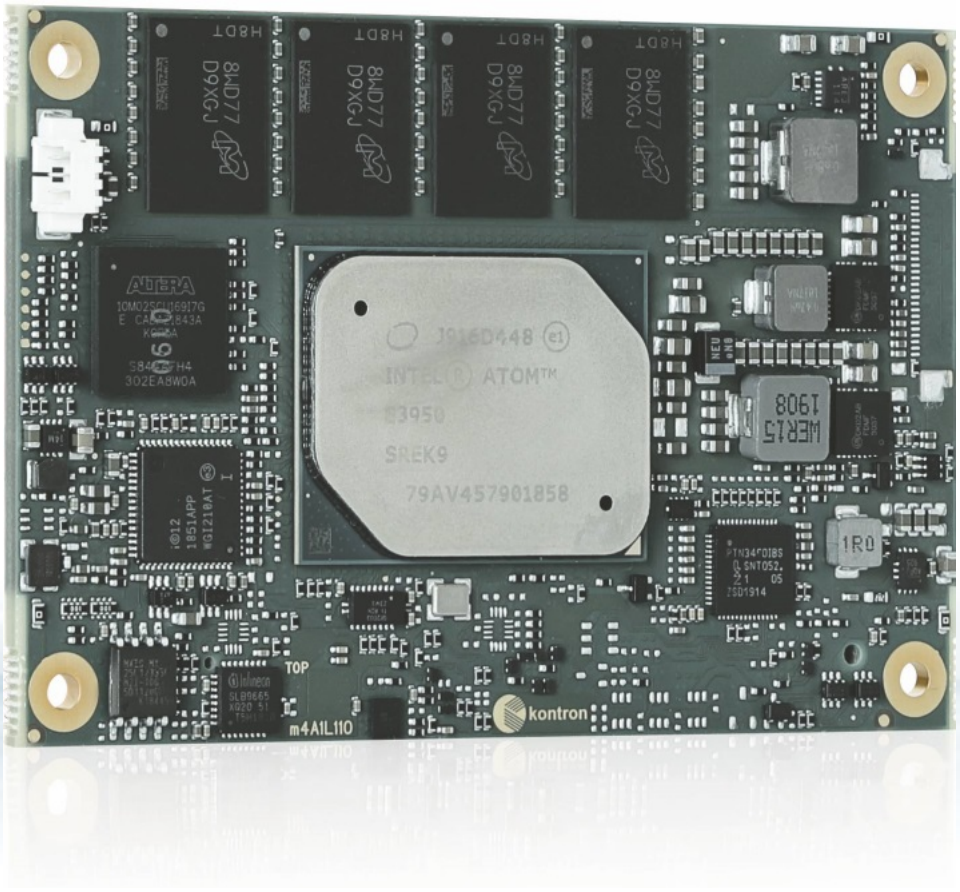
USER GUIDE



COMe-m4AL10

Doc. User Guide, Rev. 1.4

Doc. ID: 1065-8037

This page has been intentionally left blank

COME-M4AL10 - 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.

This user guide is protected by copyright. All rights are reserved by Kontron. No part of this document may be reproduced, transmitted, transcribed, stored in a retrieval system, or translated into any language or computer language, in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise), without the express written permission of Kontron. Kontron points out that the information contained in this user guide is constantly being updated in line with the technical alterations and improvements made by Kontron to the products and thus this user guide only reflects the technical status of the products by Kontron at the time of publishing.

Brand and product names are trademarks or registered trademarks of their respective owners.

©2019 by Kontron Europe GmbH

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	2019-Nov-05	CW
1.1	Removed the Power (Max.) from Table 6	2019-Dec-17	CW
1.2	N3350 changed to N3350E and N4200 changed to N4200E, memory channel information changed to 1 channel, PCI express lanes redefined and eMMC 5.1 NAND Flash included.	2020-Mar-16	CW
1.3	Extended Specification of COMe-m4AL10 Processor Variants Table 5	2020-May-14	CW
1.4	Changed Pin-B99 DDI0CTRLDATA_AUX-, to a Pull up (PU) resistor, company name and address. Added electrical spec cautions	2021-July-15	CW

Terms and Conditions

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

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

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

Customer Support

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

Customer Service

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

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

Customer Comments

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

Symbols

The following symbols may be used in this user guide

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

For Your Safety

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

High Voltage Safety Instructions

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

⚠CAUTION

Warning

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

⚠CAUTION

Electric Shock!

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

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

Special Handling and Unpacking Instruction

NOTICE

ESD Sensitive Device!

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

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

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

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

Lithium Battery Precautions

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

⚠CAUTION

Danger of explosion if the battery is replaced incorrectly.

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

General Instructions on Usage

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

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

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

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

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

Quality and Environmental Management

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

Disposal and Recycling

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

WEEE Compliance

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

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

Environmental protection is a high priority with Kontron.

Kontron follows the WEEE directive

You are encouraged to return our products for proper disposal.

Table of Contents

Symbols **6**
For Your Safety **7**
High Voltage Safety Instructions 7
Special Handling and Unpacking Instruction 7
Lithium Battery Precautions 8
General Instructions on Usage **8**
Quality and Environmental Management **8**
Disposal and Recycling 8
WEEE Compliance 8
Table of Contents **9**
List of Tables **11**
List of Figures **12**
1/ Introduction **13**
1.1. Product Description 13
1.2. Product Naming Clarification 14
1.3. COM Express® Documentation 14
1.4. COM Express® Functionality 15
1.5. COM Express® Benefits 15
2/ Product Specification **16**
2.1. Module Variants 16
2.1.1. Commercial Grade Modules (0°C to +60°C) 16
2.1.2. Industrial Temperature Grade Modules (E2, -40°C to +85°C) 16
2.2. Accessories 17
2.3. Functional Specification 18
2.3.1. Block Diagram 18
2.3.2. Processors 19
2.3.3. Platform Controller Hub (PCH) 20
2.3.4. System Memory 20
2.3.5. Digital Display Interfaces (DP/HDMI/DVI) 20
2.3.6. LVDS 21
2.3.7. HD Audio 21
2.3.8. PCI Express (PCIE) Lanes [0-3] 21
2.3.9. USB 22
2.3.10. SATA 22
2.3.11. Ethernet LAN (option) 23
2.3.12. COMe High-speed Serial Interfaces Overview 23
2.3.13. Storage 24
2.3.14. BIOS/Software Features 24
2.3.15. COMe Specification Features 24
2.3.16. Special Features 24
2.3.17. Optional Features 25
2.4. Power Specification 26
2.4.1. Power Supply Specification 26
2.4.2. Power Management 27
2.4.3. Power Supply Control Settings 27
2.4.4. Power Supply Modes 28
2.5. Thermal Management 30

2.5.1. Heatspreader Plate (HSP) Assembly and Metal Heat Slug 30
2.5.2. Active/Passive Cooling Solutions 30
2.5.3. Operating with Kontron Heatspreader Plate (HSP) Assembly 30
2.5.4. Operating without Kontron Heatspreader Plate (HSP) Assembly 30
2.5.5. Temperature Sensors 31
2.5.6. On-board Fan Connector 32
2.6. Environmental Specification 32
2.6.1. Humidity 33
2.7. Standards and Certifications 33
2.7.1. MTBF 33
2.8. Mechanical Specification 35
2.8.1. Module Dimensions 35
2.8.2. Module Height 35
2.8.3. Heatspreader and Metal Heat Slug Dimensions 36
3/ Features and Interfaces 37
3.1. ACPI Power States 37
3.2. APPROTECT Security Solution (option) 37
3.3. eMMC Flash Memory (option) 38
3.4. Fast I2C 38
3.5. GPIO 38
3.6. Hardware Monitor 38
3.7. LPC 39
3.8. Real Time Clock (RTC) 39
3.9. Serial Peripheral Interface (SPI) 39
3.9.1. SPI boot 40
3.9.2. Using an External SPI Flash 40
3.9.3. External SPI Flash Boot on Modules with Intel® Management Engine 41
3.10. SpeedStep™ Technology 41
3.11. SD Card 41
3.12. Trusted Platform Module (TPM 2.0) 42
3.13. UART 42
3.14. Watchdog Timer – Dual stage (WTD) 42
3.14.1. Watchdog Timer Signal 43
3.15. XDP Debug Port (option) 43
4/ System Resources 44
4.1. Interrupt Request (IRQ) Lines 44
4.2. Memory Area 44
4.3. I/O Address Map 45
4.4. Peripheral Component Interconnect (PCI) Devices 46
4.5. I2C Bus 46
4.6. System Management (SM) Bus 46
5/ COMe Interface Connector 48
5.1. Connecting the COMe Interface Connector to the Carrier Board 49
5.2. X1A Signals 49
5.3. COMe Interface Connector (X1A) Pin Assignment 50
5.4. Connector X1A Row A1 - A110 50
5.5. Connector X1A Row B1 – B110 54
6/ UEFI BIOS 58
6.1. Starting the uEFI **BIOS** 58

6.2. Navigating the uEFI BIOS 58
6.3. Getting Help 59
6.4. Setup Menus 59
6.4.1. Main Setup Menu 60
6.4.2. Advanced Setup Menu 61
6.4.3. Chipset Setup Menu 68
6.4.4. Security Setup Menu 70
6.4.5. Boot Setup Menu 72
6.4.6. Save and Exit Setup Menu 73
6.5. The uEFI Shell 74
6.5.1. Entering the uEFI Shell 74
6.5.2. Exiting the uEFI Shell 74
6.6. uEFI Shell Scripting 75
6.6.1. Startup Scripting 75
6.6.2. Create a Startup Script 75
6.6.3. Example of Startup Scripts 75
6.7. Firmware Update 75
6.7.1. Firmware Updating Procedure 75
7/ Technical Support 77
7.1. Returning Defective Merchandise 77
8/ Warranty 78
8.1. Limitation/Exemption from Warranty Obligation 78
Appendix A: List of Acronyms 79
About Kontron – Member of the S&T Group 81

List of Tables

Table 1: Type 10 and COMe-m4AL10 Functionality 15
Table 2: Product Number for Commercial Grade Modules (0°C to +60°C operating) 16
Table 3: Product Number for Industrial Grade Modules (-40°C to +85°C operating) 16
Table 4: Accessories 17
Table 5: Specification of COMe-m4AL10 Processor Variants 19
Table 6: COMe-m4AL10 Power Supply Voltage Requirements 26
Table 7: Power Supply Control Settings 27
Table 8: ATX Mode Settings 28
Table 9: Single Power Supply Mode Settings 29
Table 10: Heatspreader Temperature Specifications 30
Table 11: Fan Connector (3-Pin) Pin Assignment 32
Table 12: Electrical Characteristics of the Fan Connector 32
Table 13: Temperature Grade Specifications 32
Table 14: Humidity Specification 33
Table 15: Standards and Certifications 33
Table 16: MTBF 34
Table 17: Supported Power States Function 37
Table 18: Supported BIOS Features 39
Table 19: SPI Boot Pin Configuration 40
Table 20: Supported SPI Boot Flash Types for 8-SOIC Package 40
Table 21: SDIO Interface Signal Relationship to GPIO 42
Table 22: Dual Staged Watchdog Timer- Time-Out Events 43
Table 23: Interrupt Requests 44
Table 24: Designated Memory Location 44
Table 25: Designated I/O Port Address 45

Table 26: I2C Bus Port Address 46
Table 27: SMBus Address 47
Table 28: General Signal Description 49
Table 29: Connector X1A Row A1 to A110 Pin Assignment 50
Table 30: Connector X1A Row B1 to B110 Pin Assignment 54
Table 31: Navigation Hot Keys Available in the Legend Bar 58
Table 32: Main Setup Menu Sub-screens and Functions 60
Table 33: Advanced Setup menu Sub-screens and Functions 61
Table 34: Chipset Set > North Bridge Sub-screens and Function 68
Table 35: Chipset Set> South Bridge Sub-screens and Functions 69
Table 36: Security Setup Menu Sub-screens and Functions 70
Table 37: Boot Setup Menu Sub-screens and Functions 72
Table 38: Save and Exit Setup Menu Sub-screens and Functions 73
Table 39: List of Acronyms 79

List of Figures

Figure 1: COMe-m4AL10 Front Side 13
Figure 2: Block Diagram COMe-m4AL10 18
Figure 3: SoC Temperature Sensor 31
Figure 4: Module Temperature Sensor 31
Figure 5: Fan Connector 3-Pin 32
Figure 6: MTBF De-rating Values 34
Figure 7: Module Dimensions 35
Figure 8: Module and Carrier Height 35
Figure 9: Heatspreader and Metal Heat Slug Dimensions 36
Figure 10: COMe Interface Connector (X1A) with 220 pins 48
Figure 11: COMe-m4AL10 Bottom Side 48
Figure 12: Setup menu Selection Bar 59
Figure 13: Main Setup Menu Screen 60
Figure 14: Advanced Setup Menu Screen 61
Figure 15: Chipset > North Bridge Menu Screen 68
Figure 16: Chipset>South Bridge Menu Initial Screen 69
Figure 17: Security Setup Menu Screen 70
Figure 18: Boot Setup Menu Screen 72
Figure 19: Save and Exit Setup Menu Screen 73

1/ Introduction

This user guide describes the COMe-m4AL10 made by Kontron and focuses on describing the COMe-m4AL10's special features. New users are recommended to study this user guide before switching on the power.

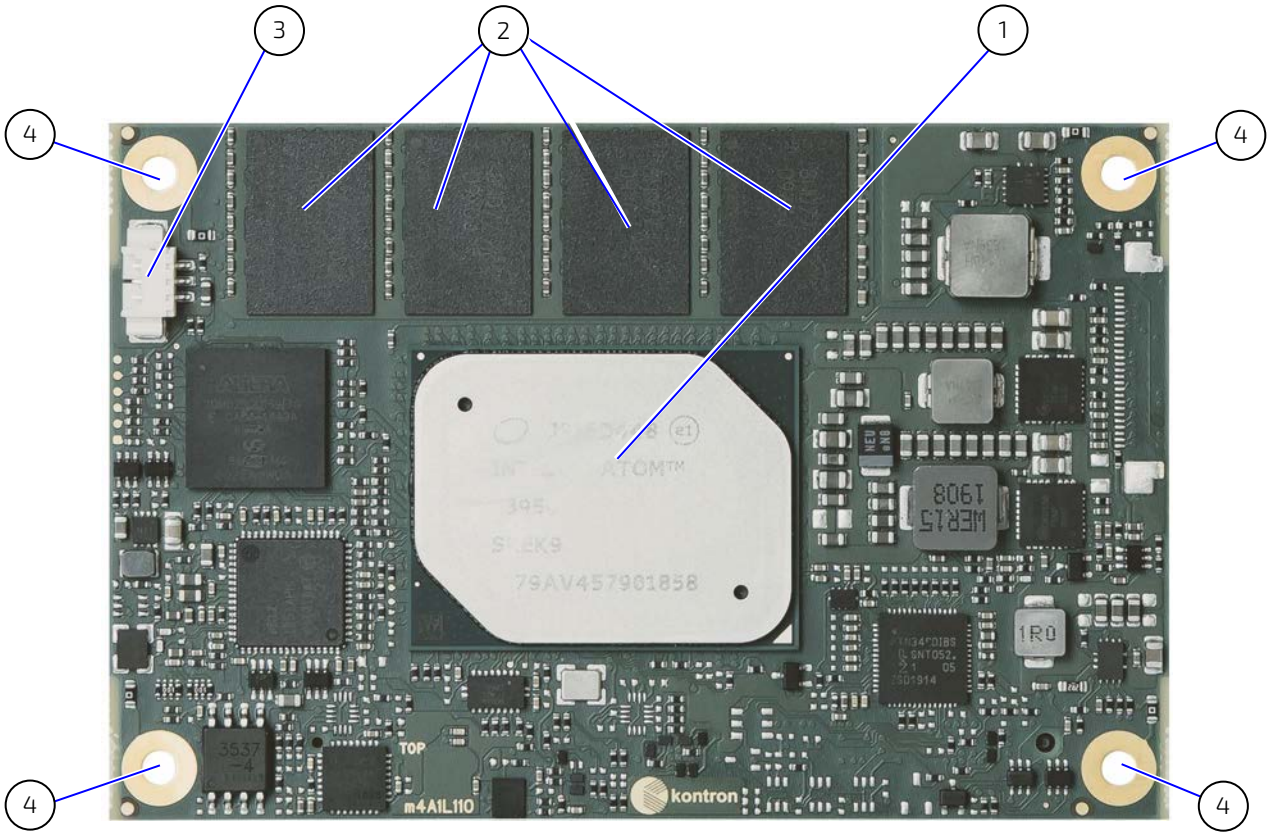
1.1. Product Description

The COMe-m4AL10 is small form factor COM Express® type 10 Computer-On-Module designed for flexible implementation within multiple embedded industrial environments. Based on the Intel® Apollo Lake® series of processors Atom™, Pentium® and Celeron®, with an integrated chipset (SoC) the COMe-m4AL10 combines increased efficiency and performance with TDP as low as 6 W and no more than 12 W, with Intel's® extensive HD Graphics capabilities.

Key COMe-m4AL10 features are:

- Intel® Apollo Lake® processors with integrated chipset
- Small form factor COM Express® mini type 10 pinout, compatible with the PICMG COM.0 Rev 2.1 spec.
- Up to 16 GByte LPDDR4 memory down (non-ECC)
- High-speed connectivity 4x PCI Express, 1x 1 Gb Ethernet, 2x USB 3.0/2.0 + 6x USB 2.0, 2x SATA Gen.3
- Support for Industrial and commercial temperature grade environments

Figure 1: COMe-m4AL10 Front Side



1 SoC
2 4x memory down
3 3-pin fan connector
4 4x mounting points for standoffs

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)
- Intel's processor code name
  - AL = Apollo Lake
- Pinout type
  - Type 10
  - Type 7
  - Type 6
- Available temperature variants
  - Commercial
  - Extended (E1)
  - Industrial (E2)
  - Screened industrial (E2S)
- Processor Identifier
- Chipset identifier (if chipset 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-m4AL10 Functionality

Feature	Type 10	COMe-m4AL10
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 3.0/2.0 6x USB 2.0
LVDS (eDP)	1x single 24-bit channel	1x single 24-bit channel LVDS with eDP overlay option
DP++ (DP/HDMI/DVI)	1x	1x
SPI	1x	1x
LPC	1x	1x
External SMB	1x	1x
I2C	1x	1x (internal)
GPIO or SDIO	8x 1x optional	8x 1x SD card interface
UART (2-wire COM)	2x	2x
TPM	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

2.1. Module Variants

The COMe-m4AL10 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.

2.1.1. 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
34010-0204-11-2	COMe-m4AL10 N3350E 2G/4S	COM Express® mini pin-out type 10 with Intel® Celeron® N3350E, 2GB LPDDR4-2133 memory down, 4GB eMMC pSLC, commercial temperature
34010-0416-11-4	COMe-m4AL10 N4200E 4G/16S	COM Express® mini pin-out type 10 with Intel® Pentium® N4200E, 4GB LPDDR4-2400 memory down, 16GB eMMC pSLC, 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
34011-0200-13-5	COMe-m4AL10 E2 E3930 2G	COM Express® mini pin-out type 10 Computer-on-Module with Intel® Atom™x5 E3930, 2GB LPDDR4-2133 memory down, industrial temperature
34011-0408-13-5	COMe-m4AL10 E2 E3930 4G/8S	COM Express® mini pin-out type 10 with Intel® Atom™x5 E3930, 4GB LPDDR4-2133 memory down, 8GB pSLC eMMC, industrial temperature
34011-0400-16-5	COMe-m4AL10 E2 E3940 4G	COM Express® mini pin-out type 10 with Intel® Atom™x5 E3940, 4GB LPDDR4-2133 memory down, industrial temperature
34011-0416-16-5	COMe-m4AL10 E2 E3940 4G/16S	COM Express® mini pin-out type 10 with Intel® Atom™x5 E3940, 4GB LPDDR4-2133 memory down, 16GB eMMC pSLC, industrial temperature
34011-0832-16-7	COMe-m4AL10 E2 E3950 8G/32S	COM Express® mini pin-out type 10 with Intel® Atom™x7 E3950, 8GB LPDDR4-2400 memory down, 32GB eMMC pSLC, industrial temperature

2.2. Accessories

Accessories are either product specific, COMe-type 10 specific, or general COMe accessories. For more information, contact your local Kontron Sales Representative or Kontron Inside Sales.

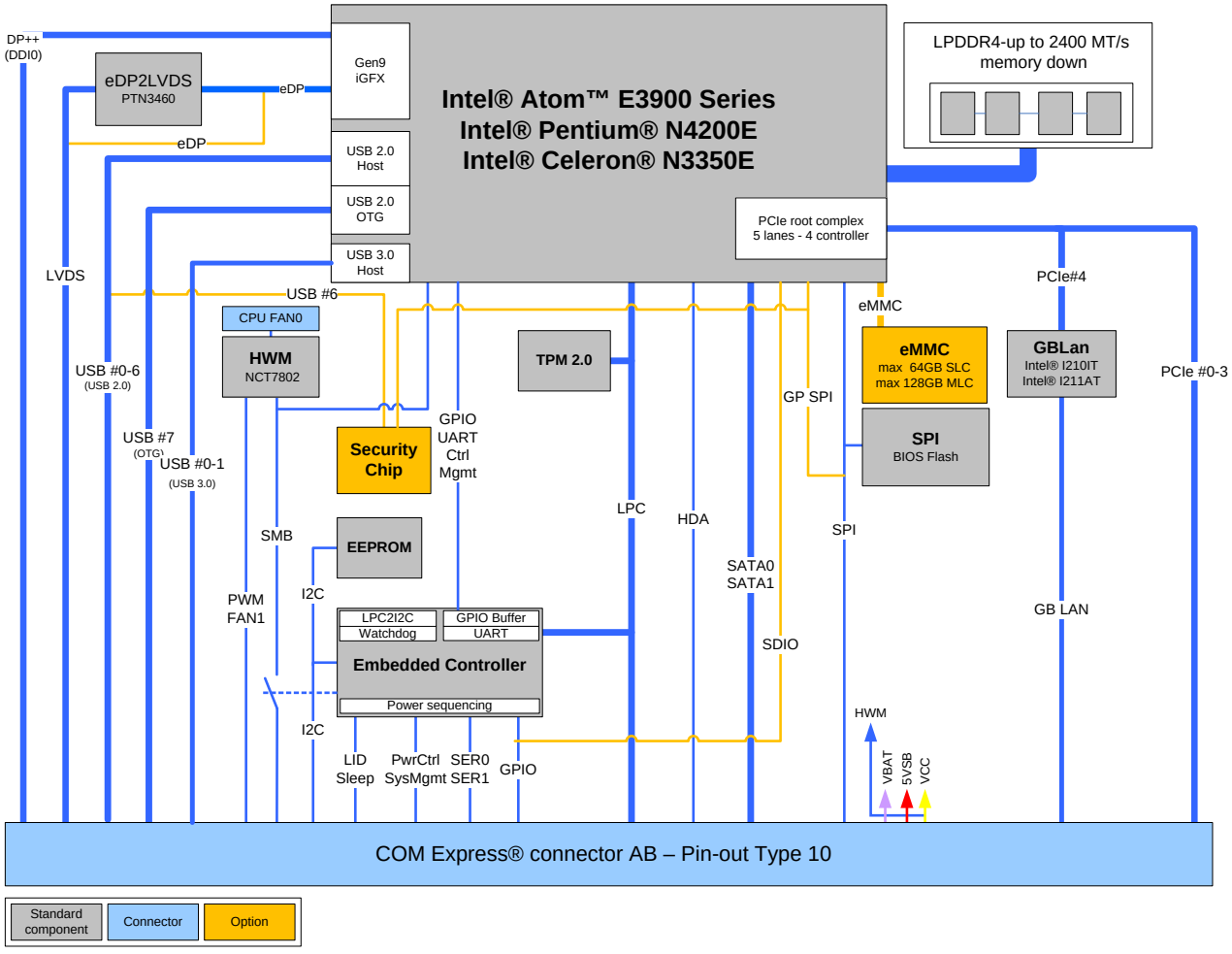
Table 4: Accessories

Part Number	Heatspreader	Description
34101-0000-00-2	COMe Eval Carrier2 T10	COM Express® Evaluation Carrier Type 10
34105-0000-00-x	COMe Ref.Carrier-i T10 TNIx	COM Express® Reference Carrier Type 10 for industrial temperature (Note x= Professional -0 / Value -1 / Entry -2)
34009-0000-99-2	HSP COMe-m(4)AL10 (E2) Slim Thread	Slim line heatspreader 6.5mm for COMe-m(4)AL10 commercial and E2, threaded mounting holes
34009-0000-99-3	HSP COMe-m(4)AL10 (E2) Slim Through	Heatspreader for COMe-m(4)AL10 commercial and E2, threaded mounting holes
34009-0000-99-0	HSP COMe-m(4)AL10 (E2) Thread	Heatspreader for COMe-m(4)AL10 commercial and E2, through holes
34009-0000-99-1	HSP COMe-m(4)AL10 (E2) Through	Heatspreader for COMe-m(4)AL10 commercial and E2, through holes
34099-0000-99-0	COMe mini Active Uni Cooler	COM Express® mini Universal Active Cooler for Heatspreader Mounting (for CPUs <10W)
34099-0000-99-1	COMe mini Passive Uni Cooler	COM Express® mini Universal Passive Cooler for Heatspreader Mounting
34099-0000-99-3	COMe mini Passive Uni Cooler Slim Top Mount	COM Express® mini Universal Passive Cooler Slim for Heatspreader Top Mounting

2.3. Functional Specification

2.3.1. Block Diagram

Figure 2: Block Diagram COMe-m4AL10



2.3.2. Processors

The Intel® Apollo Lake® series of processors Atom™, Pentium® and Celeron® use the 14 nm process technology, with a compact 24 mm x 31 mm package size, FCBGA 1296.

The processors variants support the following technologies:

- Intel® 64 Architecture
- Idle States
- Intel® Virtualization Technology (VT-x)
- Intel® Virtualization Technology for Directed I/O (VT-d)
- Secure Boot
- Enhanced Intel Speedstep® Technology
- Thermal Monitoring Technologies
- Intel® HD Audio Technology
- Intel® Identity Protection Technology
- Intel® AES New Instructions
- Secure Key

The following table lists the processor specifications compatible with the COMe-m4AL10.

Table 5: Specification of COMe-m4AL10 Processor Variants

Intel®	Atom™	Atom®	Atom™	Pentium®	Celeron®
	x7 E3950	x5 E3940	x5 E3930	N4200E	N3350E
# of Cores	4	4	2	4	2
# of Threads	4	4	2	4	2
Processor Base Frequency	1.6 GHz	1.6 GHz	1.3 GHz	1.1 GHz	1.1 GHz
Burst Frequency	2 GHz	1.8 GHz	1.8 GHz	2.5 GHz	2.4 GHz
GPU EU#	18	12	12	18	12
Thermal Design Power (TDP)	12 W	9.5 W	6.5 W	6 W	6 W
Memory Types	LPDDR4-2133/2400	LPDDR4 -2133	LPDDR4 -2133	LPDDR4-2133/2400	LPDDR4-2133/2400
Max. # Memory Channels	2[1]	2[1]	2[1]	2[1]	2[1]
Max. Memory Size	8 GB	8 GB	8 GB	8 GB	8 GB
Max. Memory Bandwidth	25.60 GB/s	25.60 GB/s	25.60 GB/s	29.86 GB/s	29.86 GB/s
ECC Memory	Supported	Supported	Supported	Not supported	Not supported
Graphics	HD Graphics 505	HD Graphics 500	HD Graphics 500	HD Graphics 505	HD Graphics 500

Intel®	Atom™	Atom®	Atom™	Pentium®	Celeron®
	x7 E3950	x5 E3940	x5 E3930	N4200E	N3350E
Max. # PCIe Devices	4	4	4	4	4
Use Condition	Embedded Broad Marketing Extended Temp. Industrial Extended Temp [2]			PC/Client	

[1] Depending on the number of accommodated memory chips 1 or 2 memory channels are used.

[2] The default configuration for the Atom® processor E3900 series is for use condition "Embedded Broad Market Extended Temp".

Contact Kontron support if you want to use the Atom® processor E3900 series in use condition "Industrial Extended Temp" for 24/7 usage.

Detailed information about the various use condition definitions for the Atom® processor E3900 series is available from Intel under NDA

2.3.3. Platform Controller Hub (PCH)

The Intel® Apollo Lake® series of processors Atom™, Pentium® and Celeron® are a System on Chip (SoC) solution, including an integrated PCH.

2.3.4. System Memory

The COMe-m4AL10 supports LPDDR4 memory down configuration with a capacity of up to 16 GByte. The maximum data transfer rate is 2400 MT/s for industrial and commercial temperature graded variants.

The following table lists specific system memory features:

Memory Down	4GByte, 8GByte and 16 GByte – LPDDR4
Peak Bandwidth	38.4 GB/s

2.3.5. Digital Display Interfaces (DP/HDMI/DVI)

The Digital Display Interface (DDI0) supports dual-mode Display Port (DP) 1.2 (++). The dual-mode DP supports two independent displays on DDIO and the use of DP to HDMI or DP to DVI-D passive adapters. In total, a maximum of three independent displays are possible if including LVDS.

The following table lists the maximum display resolution of the supported DDIO.

Display Interfaces	Maximum Resolution
DP 1.2 (++)	4096 x 2160 @ 60 Hz
HDMI 1.4	3840 x 2160 @ 30 Hz
DVI-D	3840 x 2160 @ 30 Hz

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

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

2.3.6. LVDS

The LVDS channel supports a 24-bit LVDS panel. The eDP to LVDS bridge is only necessary for LVDS support and can be removed if LVDS signals are optionally overlaid with eDP signals.

The following table lists the LVDS features.

LVD Channels	1x
LVDS Bits/Pixel	24-bit color
LVDS/eDP Maximum Resolution	4096 x 2160 @ 60Hz
PWM Backlight Control	Supported
Supported Flat Panels	EDID / JILI / DisplayID

2.3.7. HD Audio

The HD Audio link supports one audio device.

The following table lists the Audio features.

Type	Intel® High Definition (HD) Audio
# Audio Devices	1 x

2.3.8. PCI Express (PCIE) Lanes [0-3]

The Intel® Apollo Lake® processor supports a maximum of six PCIe lanes. However, only four PCIe root ports for four PCIe devices are provided.

The COMe-m4AL10 supports five PCIe lanes as follows:

- 4x COMe lanes PCIe[0-3]
- 1x lane for GBE0_MDI#

The five available high-speed PCI Express Gen 2.0 lanes support the PCIe lane configuration options:

- 4 x1 (default) 3 x1 for COMe lanes PCIe lanes PCIe[0-3] + 1 x1 for onboard LAN
  or 4 x1 for COMe lanes PCIe lanes PCIe[0-3] no onboard LAN
- 2 x1 + 1 x2 / 2 x2 / 1 x4 for COMe lanes PCIe lanes PCIe[0-3] + 1 x1 for onboard LAN

The following table lists the possible PCI Express lane configurations.

COMe Connector	SoC Port	Configuration 1	Configuration 2	Configuration 3	Configuration4
		4 x1 (default)	2 x1 + 1 x2	2 x2	1 x4
PCIE_0	PCIe #0	x1	x2	x2	x4
PCIE_1	PCIe #1	x1			
PCIE_2	PCIe #2	x1	x1	x2	
PCIE_3	PCIe #3	x1	x1		
GBE0_MDI#	PCIe #4	LAN[1]	LAN	LAN	LAN

[1] In configuration 1, If LAN is implemented only three external PCIe devices can be used at the same time as LAN uses one of the four PCIe root ports.

The various PCIe lane configurations require different BIOS versions and users may be required to flash a new BIOS version to change the PCIe lane configuration:

- Configuration 1 – default setting in BIOS
- Configuration 2 & 4 – BIOS versions are available in Kontron's Customer Section
- Configuration 3 – For information, contact Kontron support

2.3.9. USB

The eight USB ports are configured as six dedicated USB 2.0 ports and two dual USB 3.0/2.0 ports

The following table lists the supported USB features.

USB Ports	2x USB 3.0 (USB 3.0/USB 2.0 compatible) 6x USB 2.0
USB Over Current Signals	2x
USB Client Port	1x (COMe port 7 can be configured as client port)

The COMe USB port 7 is a dual role (Client /Host). When Kontron's security chip is connected SOC port 7, the COMe USB 2.0 port 6 is not available.

The following table shows the COMe connector to SoC High-speed I/O port relationship for USB 3.0/USB 2.0

COMe Connector	SoC Port	USB 2.0	USB 3.0	Description
USB0	USB2_#1	✓	✓	Optional connection for USB 3.0 dual role
USB1	USB2_#2	✓		
USB2	USB2_#3	✓		
USB3	USB2_#4	✓		
USB4	USB2_#5	✓		
USB5	USB2_#6	✓		
USB6	USB2_#7	✓		Optional Kontron security chip, connects to SoC port 7. COMe USB 2.0 port 6 is not available with this option
USB7	USB2-#0	✓	✓	USB 2.0 dual role (Client/Host) Optional connection for USB 3.0 dual role

2.3.10. SATA

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

The following table shows the COMe connector to SoC High-speed I/O port relationship for SATA.

COMe Connector	SoC I/O Port	Description
SATA_0	SATA #0	SATA Gen.3, 6 Gb/s
SATA_1	SATA #1	SATA Gen.3, 6 Gb/s

2.3.11. Ethernet LAN (option)

The Ethernet Controller supports one Gigabit Ethernet (1GbE) connectivity,and includes physical layer (PHY) ports supporting Ethernet Media Dependent Interfaces (MDI) MDI[0-3]. The Ethernet controllers Intel®i210 or Intel®i211 are used, depending on whether the industrial or commercial temperature grade is required.

If LAN is implemented, only three external PCIe devices can be used at the same time as LAN uses one of the four PCIe root ports.

The following table lists the supported Ethernet features.

Ethernet	10/100/1000 Mbit
Ethernet Controller	Intel ® i211 (commercial temperature) Intel® i210 (industrial temperature)

Some additional features of the Intel® i210 and i211 Ethernet controllers are:

- Energy Efficient Ethernet (IEEE 802.3az)
- Jumbo frames (up to 9 kB)
- Interrupt moderation, VLAN support, IP checksum
- RSS and MSI-X to lower CPU utilization in multi-core systems
- Advanced cable diagnostics, auto MDI-X
- Error correcting memory (ECC)
- IEEE1588/802.1AS precision time synchronization for Time Sensitive Networking (TSN) applications

2.3.12. COMe High-speed Serial Interfaces Overview

The high-speed serial interfaces PCI Express Gen. 2.0, USB 3.0, SATA Gen.3 and 1 GBE are available on the COM Express® 220-pin connector.

The following table shows the COMe connector to SoC High-speed I/O port relationship for all interfaces.

COMe Connector	SoC Port	PCIE	USB 3.0	SATA	GBE	Description
PCIE_0	PCIe #0	PCIe #0				PCI Express lane [0-15]
PCIE_1	PCIe #1	PCIe #1				
PCIE_2	PCIe #2	PCIe #2				
PCIE_3/	PCIe #3	PCIe #3				
GBE0_MDI#	PCIe #4				1 GbE	1 Gigabit Ethernet [1]
SATA_0	SATA #0			SATA #0		SATA Gen.3, 6 Gb/s
SATA_1	SATA #1			SATA #1		
USB_SS0	USB#_1		USB3#1			USB 3.0
USB_SS1	USB#_2	PCIE	USB3#2			

[1] If LAN is implemented, only three external PCIe devices can be used at the same time as LAN uses one of the four PCIe root ports.

2.3.13. Storage

The following table lists the supported storage features.

eMMC	1x eMMC 5.0 / 5.1 NAND Flash (option) Capacity: 2 GB to 64 GB pSLC (or 4 GB to 128 GB MLC)
SD Card	1x SD card (option)

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

2.3.14. BIOS/Software Features

The following table lists the supported BIOS and software features.

BIOS EFI	AMI Aptio V uEFI
Software	KEAPI 3 for all supported OS Linux PLD driver BIOS/ EFI Flash Utility for EFI shell, Windows 10 and Linux BIOS/EFI Utility for users to implement Boot Logo
Operating System (OS)	Windows 10 (64 bit), Yocto Linux (64 bit) and VxWorks
Custom BIOS Settings/Flash Backup	Supported

2.3.15. COMe Specification Features

The following table lists the supported COMe specification features.

SPI	Boot from an external SPI
LPC	Connected to: embedded controller and TPM
UART	2x UART (RX/TX)
LID Signals	Supported
Sleep Signals	Supported
SMBus	Connected to: HW Monitor and optional Ethernet controller
RTC	System time and date (3V max. and 10µA if modules not powered)

2.3.16. Special Features

The following table lists the supported Kontron specific product features.

External I2C	Fast I2C, MultiMaster capable
Embedded API	KEAPI3
Watchdog Support	Dual staged
TPM	TPM 2.0
Display (DDI)	4K resolutions
APPROTECT Security Solution	Kontron security chip supported on Soc port 7/COMe USB 2.0 port 6 (optional)

2.3.17. Optional Features

The following table lists the supported optional features.

PCIE	Up to four external devices
eMMC	Up to 64 GByte SLC and up to 128 GByte MLC
eDP instead of LVDS	LVDS signals can be overlaid with eDP signals
SDIO instead of GPIO	GPIO switched to SDIO to enable a SD card on the carrier
USB Client	COMe port 7 can be implemented as a USB 2.0 client

2.4. Power Specification

The COMe-m4AL10 receives power from a carrier board via the COMe Interface connector and must be connected to the carrier board to power on. The module's COMe Interface connector pins limit the amount of power received.

⚠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.

⚠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-m4AL10 uses either a wide range power supply (4.75 V to 20 V) or a +12 V single power rail nominal voltage. Other supported voltages are 5 V standby and 3.3 V RTC battery input. The COMe-m4AL10 supports operation in both single power supply mode and ATX power supply mode.

Table 6: COMe-m4AL10 Power Supply Voltage Requirements

Supply Voltage Range (VCC)	4.75 V to 20 V
Supply Voltage (VCC)	12 V
Standby Voltage	5 V ±5 %
RTC	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.

5V Standby voltage is not mandatory for operation.

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

Power management options are available within the BIOS setup. The COMe-m4AL10 implements the Advanced Configuration and Power Interface (ACPI) ACPI 5.0 hardware specification to control typical features such as power button and suspend states. If power is removed, 5 V can be applied to V_5V_STBY pins to support the suspend-states:

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

Implementing the wake-up event (S0) requires power as the module will be running.

2.4.3. 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	The PWRBTN# falling edge signal creates power button event (must be at least 50 ms (50 ms ≤ t < 4 s, typical 400 ms) at low level). 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 the 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 prevents the 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.
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 go idle before forcing a reset, even though activity is still occurring. Once the reset is asserted, it remains asserted for 5 ms to 6 ms regardless of whether the SYS_RESET# input remains asserted or not.
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	With 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".

COMe Signal	Pin	Description
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#)	B 18	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.

2.4.4. Power Supply Modes

Setting the power supply controls enables the module to operating in either:

- ATX power supply mode
- Single power supply mode.

2.4.4.1. ATX Power Supply Mode

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

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

The PS_ON# signal generated by SUS_S3# (A15) indicates that the system is in Suspend to RAM state. An inverted copy of SUS_S3# on the carrier board may be used to enable non-standby power on a typical ATX supply. The input voltage must always be higher than 5 V standby (VCC > 5 VSB) for Computer-On-Modules supporting a wide input voltage range down to 4.75 V.

The following table provides the ATX mode settings.

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.

2.4.4.2. Single Power Supply Mode

To start the module in single power supply mode connect VCC and open PWR_OK at high level. PS_ON# is not used in this mode and 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 (HSP) Assembly and Metal Heat Slug

A heatspreader plate 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 SoC 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 heatspreader plates. The optimum cooling solution depends on the COM Express® application and environmental conditions. Kontron's active or passive cooling solutions for the COMe-m4AL10 are usually 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 Specifications

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

2.5.4. Operating without Kontron Heatspreader Plate (HSP) Assembly

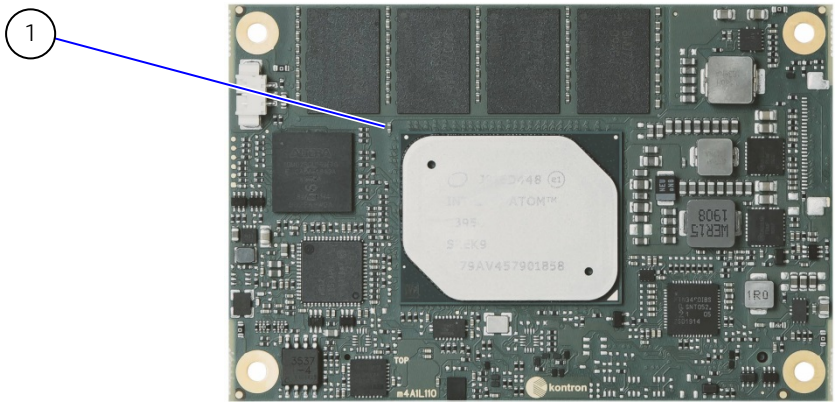
The operating temperature is the maximum measurable temperature on any spot on the module's surface.

2.5.5. Temperature Sensors

The thermal resistor (Figure 3, pos. 1) placed very close to the SoC measures the SoC 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 temperature close to the SoC. When comparing the thermal resistor value to the internal SoC 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 thermal resistor method is used to measure SoC temperature because the SoC does not support PECI based temperature measurement, and does not supply an internal diode that can be used instead of PECI. Additionally, reading the DTS based values would harm the system's real-time behavior.

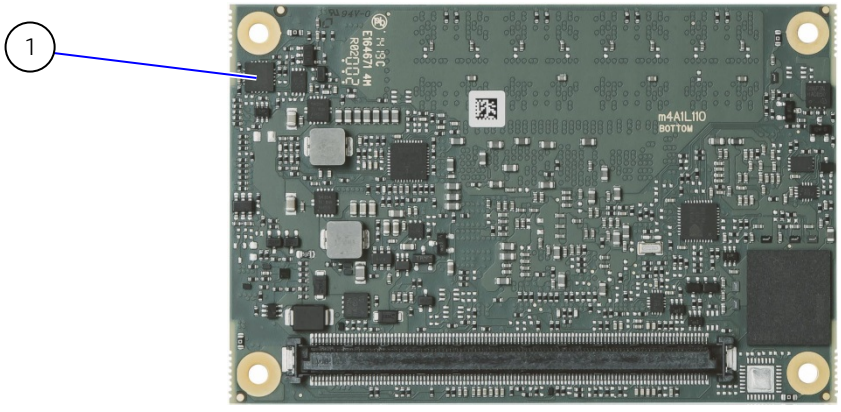
Figure 3: SoC Temperature Sensor



1 Negative Temperature Coefficient (NTC) thermal resistor measures the SoC 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). The HWM uses the SMBus interface, see Table 27: SMBus Address.

Figure 4: Module Temperature Sensor



1 Hardware Monitor (HWM) Chip measures the module temperature

2.5.6. On-board Fan Connector

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

Figure 5: Fan Connector 3-Pin

Table 11: Fan Connector (3-Pin) Pin Assignment

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

If the input voltage is below 12 V or equal to 12 V, then the maximum supply current to the on-board fan connector is 350 mA and the fan output voltage is equal to the module input voltage. The maximum supply current to the on-module fan connector is limited to 150 mA if the input voltage is 13 V but less than 20 V.

NOTICE

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

Table 12: Electrical Characteristics of the Fan Connector

Module Input Voltage (12 V and below)	
Module Input Voltage	<= 12 V
FAN Output Voltage	Equal to module's input voltage
FAN Output Current	350 mA (Max.)
Module Input Voltage (13 V and up to 20 V Max.)	
Module Input Voltage	=13 V to <=20 V
FAN Output Voltage	12 V (±10%)
FAN Output Current	Limited to 150 mA (Max.)

2.6. Environmental Specification

Kontron defines operating and non-operating temperature grades for the COMe-m4AL10. For more temperature grade information, see Chapter 2.1 Module Variants.

Table 13: Temperature Grade Specifications

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

2.6.1. Humidity

Table 14: Humidity Specification

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

2.7. Standards and Certifications

The COMe-m4AL10 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 15: Standards and Certifications

EMC		
Emission (Class B)	EN 55032 (CISPR 32)	Electromagnetic compatibility of multimedia equipment - Emission requirements
	IEC/EN 61000-6-3	Generic Emission Standard Part 6-3: Residential, commercial and light-industrial environments
Immunity (Industrial Equipment)	IEC / EN 61000-6-2	Electromagnetic compatibility (EMC) Part 6-2: Generic standards - Immunity standard for industrial environments
Safety		
Europe	EN 62368-1	Audio/video, information and communication technology equipment – Part 1: Safety Requirements
USA & Canada	UL 60950-1 / CSA 60950-1 (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 – 4000 Hz, +/- 0.15 mm, 2 g)
RoHS II	Directive 2011/65/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 calculation for the remaining parts.

The Telcordia calculation used is "Method 1 Case 3" in a ground benign, controlled environment. This particular method takes into account varying temperature and stress data and the system is assumed to have not been burned-in. Other environmental stresses (such as extreme altitude, vibration, salt-water exposure) lower MTBF values.

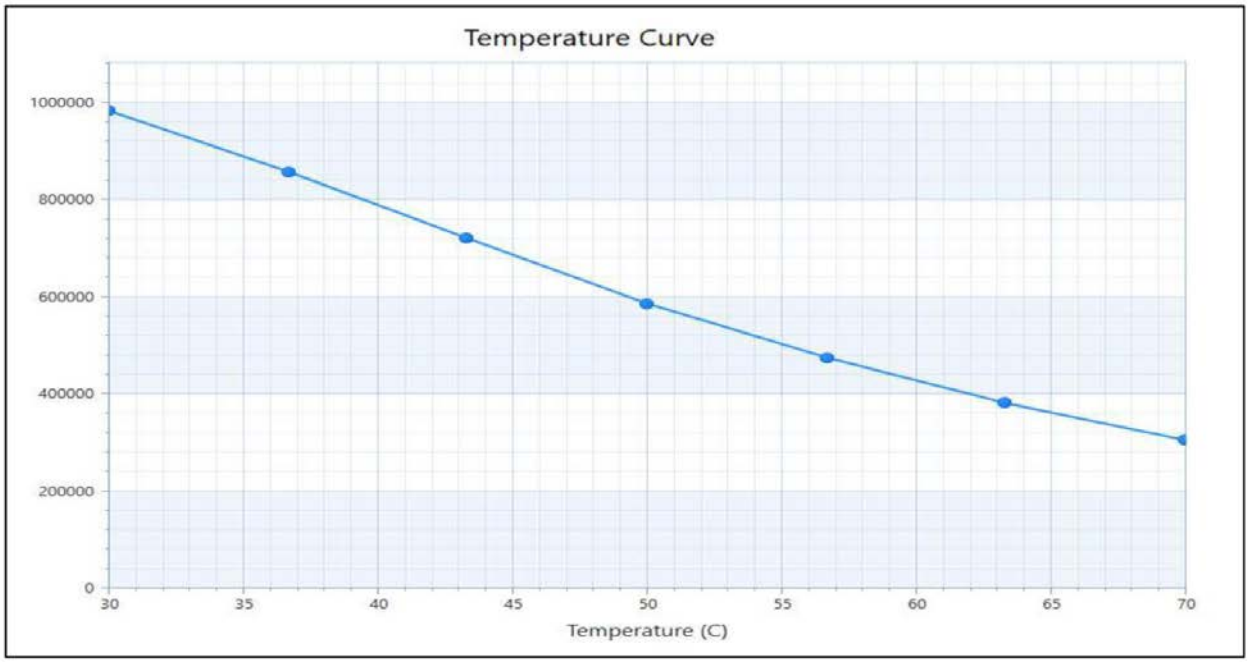
Table 16: MTBF

MTBF
System MTBF (hour) = 796297 h @ 40°C for COMe-m4AL10 E2 E3930 2G Reliability report article number: 34011-0200-13-5

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

Figure 6 shows MTBF de-rating values for commercial grade module variant 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



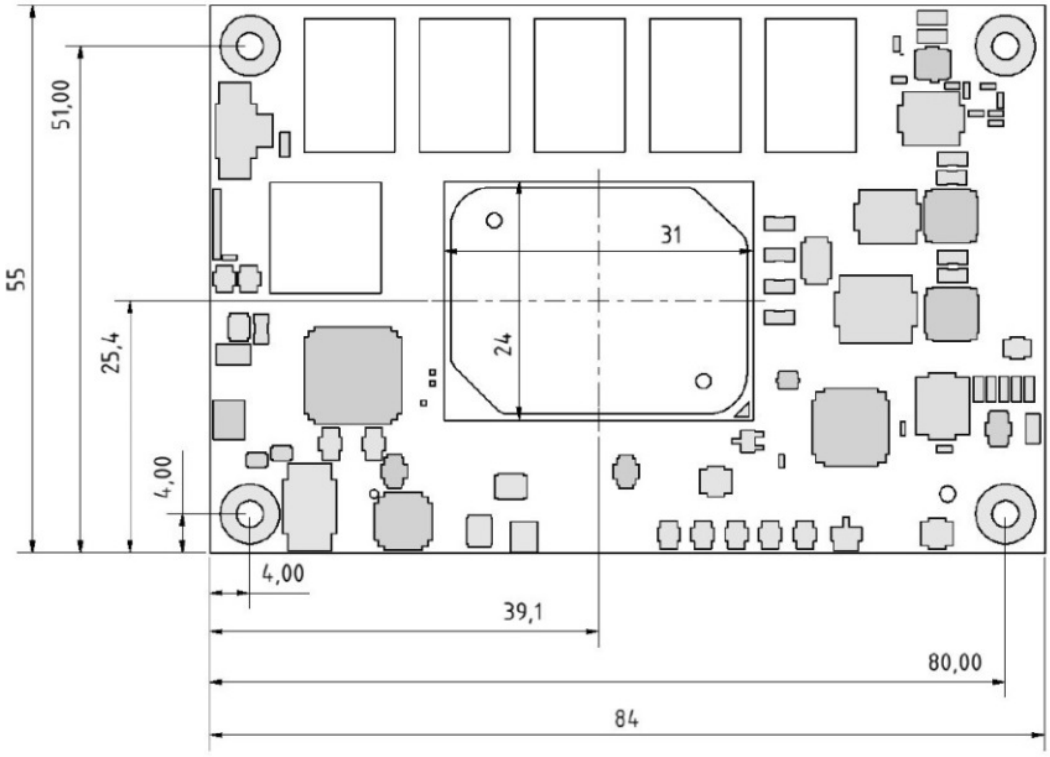
2.8. Mechanical Specification

The COMe-m4AL10 is compliant with the mechanical specification of the COM Express® PICMG COM.0 Rev 2.1.

2.8.1. Module Dimensions

The dimensions of the mini module are: 84 mm x 55 mm (3.3“x 2.17“)

Figure 7: Module Dimensions

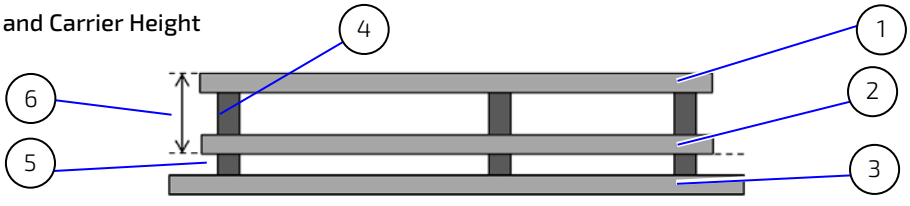


*All dimensions are in mm.

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

Figure 8: Module and Carrier Height



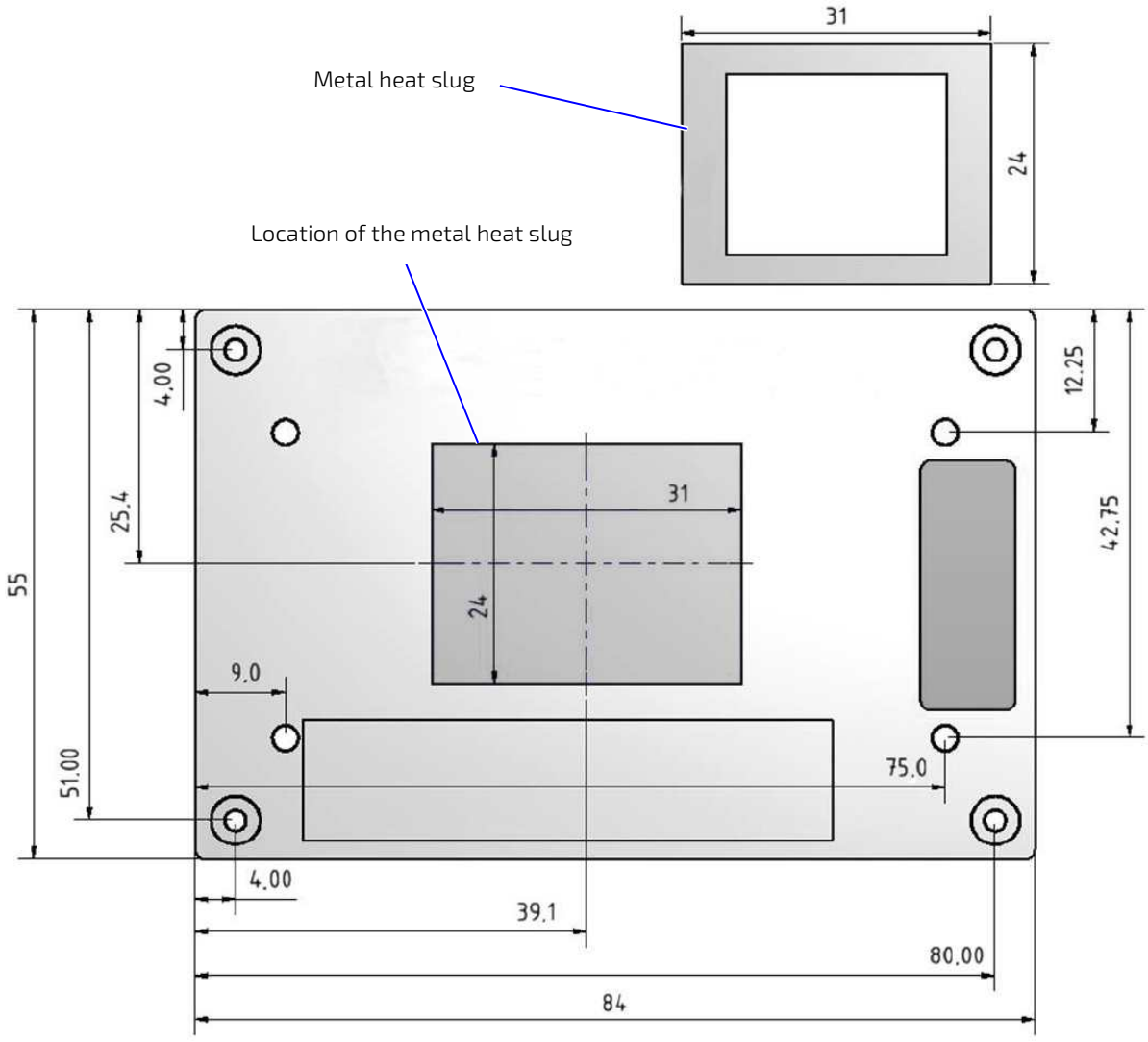
1	Heatspreader	4	Heatspreader standoff(s)
2	Module PCB board	5	Connector standoff(s) 5 mm or 8 mm
3	Carrier PCB board	6	13 mm +/- 0.65 mm

2.8.3. Heatspreader and Metal Heat Slug Dimensions

The industrial temperature grade variants include a preconfigured Intel heatspreader and therefore the metal slug, supplied in the delivery, does not have to be installed. The commercial temperature grade variants do not include a preconfigured Intel heatspreader and the metal heat slug supplied in the delivery must be installed.

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

Figure 9: Heatspreader and Metal Heat Slug Dimensions



*All dimensions shown in mm.

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-m4AL10 comes with ACPI 4.0 and supports the power states S0, S4, S5 only.

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

Table 17: Supported Power States Function

S0	Working state
S4	Suspend-to-disk/Hibernate
S5	Soft-off state

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

- Power Button
- WakeOnLan

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

- Power Button
- WakeOnLan

OS must support wake up by USB devices and the carrier board must power the USB Port with standby voltage. Depending on the Ethernet used (MAC or Phy), WakeOnLan must be enabled in the BIOS Setup and driver options.

3.2. APPROTECT Security Solution (option)

Kontron's Security Solution is a security chip for Kontron's security stack (APPROTECT). The security solution combines a software framework with an integrated security chip connected to the COMe-m4AL10's Soc port 7/COMe USB 2 port 6, and an additional (Trusted Platform Module) TPM 2.0 chip to provide comprehensive protection for the application software. Kontron APPROTECT encrypts an application's source code in a way that makes reverse engineering impossible (IP Protection/Reverse Engineering Protection).

Kontron's APPROTECT licensing additionally adds:

- License model enforcement
- Enablement of new business models by offering SDKs and software integration
- Based on time base, by counting executions or by enabling/disabling features
- Software management framework

After purchasing Kontron APPROTECT, a new firmware code for the security chip will be provided that can be installed by Kontron or by the user. If required, users can customize the solution to meet specific needs. For more information, contact Kontron Support.

3.3. eMMC Flash Memory (option)

The Embedded Multimedia Flash Card (eMMC) is eMMC 5.0 / 5.1 compatible and supports up to 64 GByte NAND Flash. During the manufacturing process, Multi Level Cell (MLC) eMMC is reconfigured to act as pseudo Single Level Cell (pSLC) eMMC to provide improved reliability, endurance and performance.

The eMMC flash memory features are:

- 2 GByte up to 64 GByte pSLC (or 4 GByte up to 128 GByte MLC)
- eMMC 5.0 /5.1 compatible

3.4. Fast I2C

The fast I2C bus supports transfer between components on the same module with data transfers up to 400 kHz. The embedded I2C controller connects to the LVS bridge and external LVDS EEPROM. The I2C bus speed is changed in the BIOS setup menu: Advanced>Miscellaneous>I2C Speed> 400kHz to 1 kHz; where 200 kHz is default.

The I2C controller supports:

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

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 on the module 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 GPIO and SDIO pins are shared. An EEPROM bit is added so that the carrier board can define if the pins are used as GPIO or SDIO. The shared 8-pins are configured in the BIOS setup as COMe-GPIO or SDIO.

Advanced>Miscellaneous>SDIO/GPIO Mode> SDIO or COMe-GPIO.

The output of the selected function is then enabled or disables in the BIOS setup option

Advanced>Miscellaneous>SDIO/GPIO Output> [Enabled, Disabled]

3.6. Hardware Monitor

The Nuvoton NCT7802Y Hardware Monitor (HWM) see Figure 4, pos.1, controls the health of the system by monitoring critical aspects such as temperatures, power supply voltages and fan speed for cooling. The HWM's internal temperature sensors measures the module's temperature. The HWM cannot read the SoC's DTS temperature. The SoC temperature is measured by the thermal resistor located close to the SoC, see Figure 3, pos.1. The HWM uses the SMBus interface, the SM bus address is set to 5C, see Table 27: SMBus Address.

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.

3.7. LPC

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

Table 18: Supported BIOS Features

Interface Signals	AMI EFI APTIO V
PS/2	Not supported
COM1/COM2	Supported as COM3 and COM4 (COM1/COM2 are already on-board)
LPT	Not supported
HWM	Not supported
Floppy	Not supported
GPIO	Not supported

Features marked as not supported do not exclude OS support, except for the HWM that is controlled by the BIOS setup within the Advanced setup menu and has no OS software support: **Advanced> H/W Monitor>**

The HWM is accessible via the System Management (SM) Bus, for more information see Chapter 4.6: System Management (SM) Bus. If any other LPC Super I/O additional BIOS implementations are necessary, contact Kontron Support.

3.8. Real Time Clock (RTC)

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 power source enabling the RTC to continue to keep time while the primary source of power is switched off or unavailable. A typical RTC voltage is 3 V with a current of less than 10 µA. If the module is powered by the mains supply, the module's RTC voltage is generated by on-module regulators, to reduce RTC current draw. The RTC's battery voltage range is 2.8 V to 3.47 V.

The RTC battery input may be left open on the carrier board if an application does not require the RTC to keep time when the main power source is off or unavailable.

3.9. 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 can only be used with a SPI Flash device to boot from the external BIOS on the carrier board.

The SPI Flash chip supports:

- Dual SPI with 2 data bits per clock cycle
- Quad SPI with 4 data bits per clock cycle
- QPI with data and command over 4 data lines

3.9.1. SPI boot

The module contains one on-module SPI Flash chip for booting and can use an external SPI chip on the carrier board for booting. It is not possible to flash a SPI Flash chip that is not the boot SPI Flash chip. The on-module SPI Flash chip is a 16 MByte, 3 V serial SPI Flash chip.

The possible SPI boot options are:

- Boot/Flash internal SPI Flash chip (module SPI Flash chip)
- Boot/Flash external SPI Flash chip (carrier board SPI Flash chip)

To configure which SPI Flash is used for booting, place jumpers on pin A34 (BIOS_DIS0#) and pin B88 (BIOS_DIS1#) as shown in Table 19: SPI Boot Pin Configuration.

Table 19: SPI Boot Pin Configuration

Configuration	BIOS_DIS0#	BIOS_DIS1#	Function
1	Open	Open	Boot on on-module SPI
2	GND	Open	Not supported
3	Open	GND	Boot on carrier board SPI
4	GND	GND	Not supported

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

Table 20: Supported SPI Boot Flash Types for 8-SOIC Package

Size	Manufacturer	Part Number	Device ID
16MB	Maxim	MX25L12835F	0x20
16MB	Macronix	W25Q128FV	0x40
16MB	Micron	N25Q128A	0xBA

3.9.2. Using an External SPI Flash

Initially, the EFI Shell is booted with an USB key containing the binary used to flash the SPI, plugged in on the system. Depending on which SPI is flashed, the (BIOS_DIS1) jumper located on the COM Express® carrier must be used.

To flash the carrier or module Flash chip:

1. Connect a SPI flash with the correct size (similar to BIOS binary (*.BIN) file size) to the carrier SPI interface.
2. Open pin A34 (BIOS_DIS0#) and connect pin B88 (BIOS_DIS1#) to ground to enable the external SPI Flash to boot on carrier SPI. (See Table 19: SPI Boot Pin Configuration)
3. Turn on the system and make sure that USB is connected then start the uEFI BIOS setup. (See Chapter 6.1: Starting the uEFI BIOS.)
4. Disable the BIOS lock.
5. Save and Exit the setup.

6. Reboot system into EFI shell.
7. From the EFI shell, enter the name of the partition of the USB Key in this example; select FS0: then press <enter>.
8. Enter the following:

```
FPT –F <biosname.BIN>
```

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

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

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

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

3.10. SpeedStep™ Technology

Intel SpeedStep™ Technology enables the adaption of high performance computing in applications by switching automatically between maximum performance mode and battery-optimized mode, depending on the needs of the application. When battery powered or running in idle mode, the processor drops to lower frequencies (by changing the processor ratios) and voltage, thus conserving battery life while maintaining a high level of performance. The frequency is automatically set back to the higher frequency, allowing users to customize performance. To use the Intel® Enhanced SpeedStep™ technology the implemented operating system must support SpeedStep™.

To achieve manual control, deactivate the SpeedStep™ feature by disabling SpeedStep™ in the BIOS Setup:

Advanced>CPU Configuration>CPU Power Management Configuration>EIST>Intel Speedstep>disable

Once disabled, manual control or modification of the processor performance is possible and uses can use third party software to control the Processor Performance States.

3.11. SD Card

The SDIO and GPIO are pin shared. An EEPROM bit is added so that the carrier board can define if the pins are used as SDIO or GPIO. The shared 8-pins are configured in the BIOS setup as SDIO or COMe-GPIO.

Advanced>Miscellaneous>SDIO/GPIO Mode> [SDIO, COMe-GPIO]

If the SDIO feature is not required, connect the GPIO directly to the COMe GPIO pins. For information regarding the relation between the SD Card interface signals and the GPIO signals see Table 21: SDIO Interface Signal Relationship to GPIO.

Table 21: SDIO Interface Signal Relationship to GPIO

COMe Signal	SD card interface signal	Description
GPI0	SD_DATA0	Bidirectional signal
GPI1	SD_DATA1	Bidirectional signal
GPI2	SD_DATA2	Bidirectional signal
GPI3	SD_DATA3	Bidirectional signal
GPO0	SD_CLK	Output from COM Express, input to SD
GPO1	SD_CMD	Output from COM Express, input to SD
GPO2	SD_WP	Input to COM Express when used as SD_WP
GPO3	SD_CD#	Input to COM Express when used as SD_CD#

3.12. Trusted Platform Module (TPM 2.0)

The TPM 2.0 chip stores RSA encryption keys specific to the host system for hardware authentication. The term TPM refers to the set of specifications applicable to TPM chips. The LPC bus connects the TPM chip to the SoC.

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

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

3.13. UART

The UART controller supports up to two serial UART ports with RX/TX signals. The COM Express® specification specifies pin A98 (SER0_TX) and pin A99 (SER0_RX) for UART0, and pin A101 (SER1_TX) and pin A102 (SER1_RX) for UART1. The UART controller is fully 16550A compatible.

UART features are:

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

3.14. Watchdog Timer – Dual stage (WTD)

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

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

The COMe-m4AL10 offers a watchdog that works with two stages that can be programmed independently, and used stage by stage.

Table 22: Dual Staged Watchdog Timer- Time-Out Events

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

3.14.1. Watchdog Timer Signal

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

3.15. XDP Debug Port (option)

The eXtended Debug Port (XDP) enables hardware debugging on the system using an optional 60-pin connector. The XDP interface includes a probe adjacent to the XDP connector and connects to the XDP connector via a ribbon cable. A remote system can then access the hardware probe to debug the system.

4/ System Resources

4.1. Interrupt Request (IRQ) Lines

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

Table 23: Interrupt Requests

IRQ	General Usage	Project Usage
0	Timer	Timer
1	Keyboard	Keyboard (Super I/O)
2	Redirected secondary PIC	Redirected secondary PIC
3	COM2	COM2
4	COM1	COM1
5	LPT2/PCI devices	One of COM3+4
6	FDD	One of COM3+4 or not used
7	LPT1	LPT1 or one of COM3+4
8	RTC	RTC
9	SCI / PCI devices	Free for PCI devices
10	PCI devices	Free for PCI devices
11	PCI devices	Free for PCI devices
12	PS/2 mouse	Free for PCI devices
13	FPU	FPU
14	IDE0	Not used
15	IDE1	Not used

4.2. Memory Area

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

Table 24: Designated Memory Location

Address Range (hex)	Size	Project Usage
00000000-0009FBFF	639 KB	Real mode memory
0009FC00-0009FFFF	1 KB	Extended BDA
000A0000-000BFFFF	128 KB	Display memory (legacy)
000C0000-000CBFFF	48 KB	VGA BIOS (legacy)
000CC000-000DFFFF	80 KB	Option ROM or XMS (legacy)
000E0000-000EFFFF	64 KB	System BIOS extended space (legacy)
000F0000-000FFFFF	64 KB	System BIOS base segment (legacy)
00100000-7FFFFFFF	128 MB	System memory (Low DRAM)
80000000-FFF00000	2 GB – 1 MB	PCI memory, other extensions (Low MMIO)
FEC00000-FEC00FFF	4 KB	IOxAPIC
FED00000-FED003FF	1 KB	HPET (Timer)
FED40000-FED40FFF	4KB	Always reserved for LPC TPM usage
FEE00000-FEEFFFFF	1MB	Local APIC region
FFFC0000-FFFFFFFF	256 KB	Mapping space for BIOS ROM/Boot vector
100000000-17FFFFFFF	2 GB	System memory (High DRAM)
180000000-F00000000	58 GB	High MMIO

4.3. I/O Address Map

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

Table 25: Designated I/O Port Address

I/O Address Range	General Usage	Project Usage
000-00F	DMA-Controller (Master) (8237)	DMA-Controller (Master) (8237)
020-021 024-025 028-029 02C-02D 030-031 034-035 038-039 03C-03D	Interrupt-Controller (Master) (8259)	Interrupt-Controller (Master) (8259)
02E-02F	SuperIO (Winbond)	External SuperIO (Winbond)
040-043 050-053	Programmable Interrupt Timer (8253)	Programmable Interrupt Timer (8253)
04E-04F	2nd SuperIO, TPM etc.	TPM
060, 064	KBD Interface-Controller (8042)	KBD Interface-Controller (8042)
061, 063 065, 067	NMI Controller	NMI Controller
062, 066	Embedded Microcontroller	Not used
070-071	RTC CMOS / NMI mask	RTC CMOS / NMI mask
072-073	RTC Extended CMOS	RTC Extended CMOS
080-083	Debug port	Debug port
0A0-0A1 0A4-0A5 0A8-0A9 0AC-0AD 0B0-0B1 0B4-0B5 0B8-0B9 0BC-0BD	Interrupt-Controller (Slave) (8259)	Interrupt-Controller (Slave) (8259)
0B2-0B3	APM control	APM control
0C0-0DF	DMA-Controller (Slave) (8237)(N/A)	Not used
0F0-0FF	FPU (N/A)	Not used
170-177	HDD-Controller IDE1 Master	Not used
1F0-1F7	HDD-Controller IDE0 Master	Not used
200-207	Gameport	Not used
220-22F	Soundblaster®	Not used
279	ISA PnP	ISA PnP
278-27F	Parallel port LPT2	Not used
295-296	Hardware monitor (Winbond default)	Reserved (If SuperIO present)
2B0-2BF	EGA	Not used
2D0-2DF	EGA	Not used
2E8-2EF	Serial port COM 4	Serial port COM4 (optional)
2F8-2FF	Serial port COM 2	Serial port COM2 from CPLD

I/O Address Range	General Usage	Project Usage
300-301	MIDI	Not used
300-31F	System specific peripherals	Not used
370-377	Floppy disk controller	Not used
376-377	HDD-Controller IDE1 Slave	Not used
378-37F	Parallel port LPT 1	LPT1 (If SuperIO present)
3BC-3BF	Parallel port LPT3	Not used
3C0-3CF	VGA/EGA	VGA/EGA
3D0-3DF	CGA	Not used
3E0-3E1	PCMCIA ExCA interface	Not used
3E8-3EF	Serial port COM3	Serial port COM3 (optional)
3F0-3F7	Floppy Disk Controller	Not used
3F6-3F7	HDD controller IDE0 Slave	Not used
3F8-3FF	Serial Port COM1	Serial port COM1
4D0-4D1	Interrupt-Controller (Slave)	Interrupt-Controller (Slave)
A80-A81	Kontron CPLD	Kontron CPLD control port
CF8	PCI configuration address	PCI configuration address
CF9	Reset control	Reset control
CFC-CFF	PCI configuration data	PCI configuration data

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

4.4. Peripheral Component Interconnect (PCI) Devices

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

4.5. I2C Bus

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

Table 26: I2C Bus Port Address

I2C Address	Used For	Available	Description
58h		No	Internally reserved
A0h	JIDA-EEPROM	No	Module EEPROM
AEh	FRU-EEPROM	No	Recommended for Baseboard EEPROM

4.6. 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 SMBus write address for all devices and the 7-bit SMBus address without bit 0.

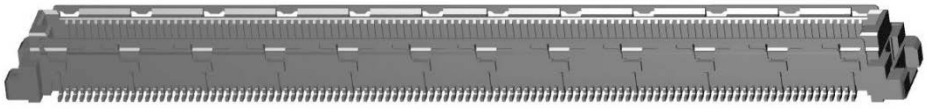
Table 27: SMBus Address

8-bit Address	7-bit Address	Device	Description	SMBus
5Ch	2Eh	HWM NCT7802Y	Do not use under any circumstances	SMB
A0h	50h	SPD DDR Channel 1 (SO-DIMM)		SMB
A4h	52h	SPD DDR Channel 2 (SO-DIMM)		SMB
30h	18h	SO-DIMM Thermal Sensor	If available on the used memory-module	SMB
34h	1Ah	SO-DIMM Thermal Sensor channel 2	If available on the used memory-module	SMB

5/ COMe Interface Connector

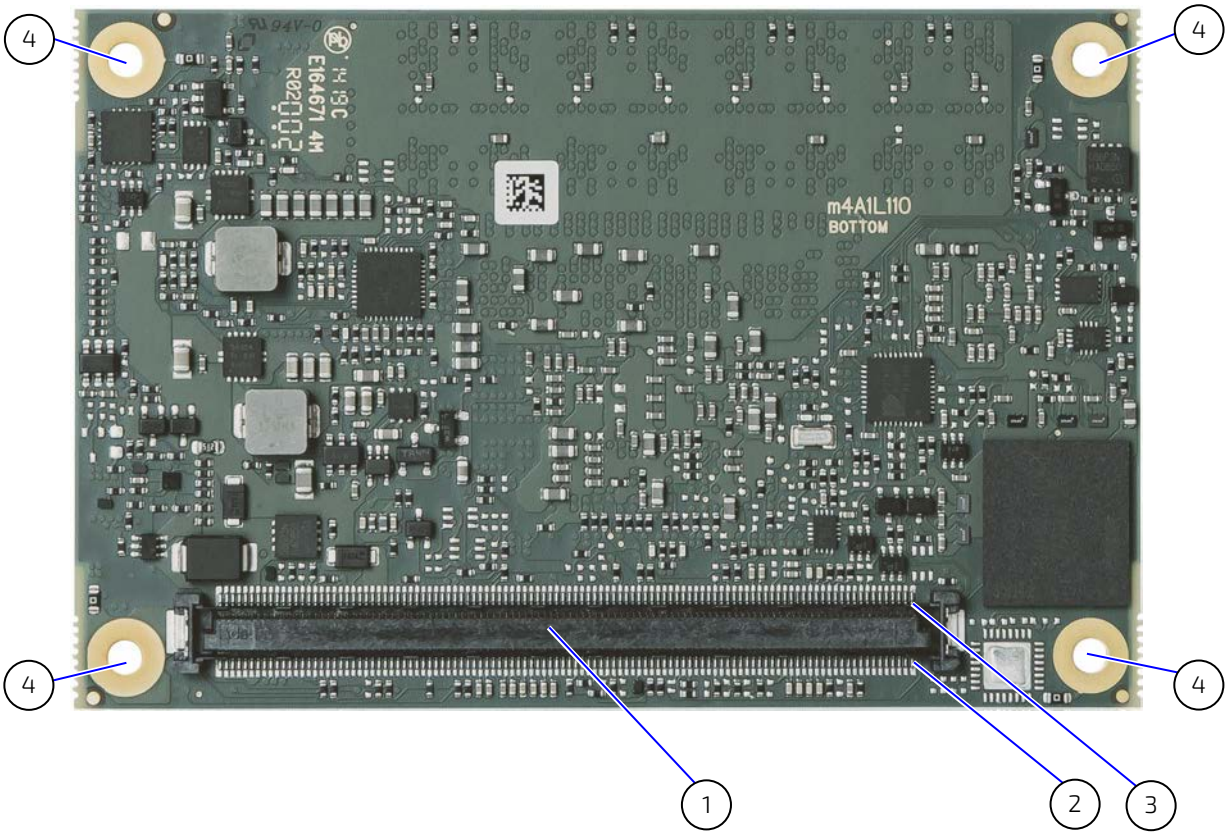
The COMe Interface connector (X1A) mounted on the bottom side of the module contains 220-pins with two rows (row A and row B), where row A contains pins A 1 to A110 and row B contains B 1 to B110.

Figure 10: COMe Interface Connector (X1A) with 220 pins



The position of the COMe interface connector (X1A) and the location of pins A1 and B1 are shown in Figure 11.

Figure 11: COMe-m4AL10 Bottom Side



1 COMe interface connector (X1A)
2 Pin A1 (seen from module's bottom side)
3 Pin B1 (seen from module's bottom side)
4 4x mounting points for standoffs

5.1. Connecting the COMe Interface Connector to the Carrier Board

The module's COMe Interface connector (X1A), mounted on the bottom side of the module, is inserted into carrier board's corresponding connector and secured using the mounting points (Figure 11, pos. 4) using either 5 mm or 8 mm standoffs, depending 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.

⚠CAUTION

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

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 28: General Signal Description. If more information is required, the Appendix at the end of this user guide and the PICMG specification COMe Rev 2.1 Type 10 standard, contain additional information.

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 28: 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

NOTICE

To protect external power lines of peripheral devices, make sure that:

- **Wires have the right diameter to withstand the maximum available current.**
- **Peripheral device enclosure fulfills the fire-protection requirements of IEC/EN60950.**

5.3. COMe Interface Connector (X1A) Pin Assignment

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

- Table 29: Connector X1A Row A1 to A110 Pin Assignment
- Table 30: Connector X1A Row B1 to B110 Pin Assignment

5.4. Connector X1A Row A1 - A110

Table 29: 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	Reference voltage for Carrier Board Ethernet magnetics center tab. The reference voltage is determined by the requirements of the Module PHY and may be as low as 0 V and as high as 3.3 V.	O		1 nF capacitor to GND
A15	SUS_S3#	Indicates Suspend to RAM (or deeper) state. An inverted copy of SUS_S3# on Carrier Board may be used to enable non-standby power on a typical ATX supply.	O-3.3	PD 10 kΩ	
A16	SATA0_TX+	SATA transmit data pair 0	DP-O		
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		
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		
A25	USB_SSRX1-	USB super speed receive data pair 1	DP-I		
A26	USB_SSRX1+				

Pin	COMe Signal	Description	Type	Termination	Description
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 determines the BIOS boot device	I-3.3	PU 10 kΩ, 3.3 V (S5)	
A35	THRMTRIP#	Thermal Trip indicates CPU has entered thermal shutdown	O-3.3	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/PU in SoC	PD 15 KΩ ±5% on downstream facing port PU 1.5 KΩ ±5% on upstream facing port
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/PU in SoC	PD 15 KΩ ±5% on downstream facing port PU 1.5 KΩ ±5% on upstream facing port
A40	USB4+				
A41	GND	Power Ground	PWR GND		
A42	USB2-	USB 2.0 data differential pair port 2	DP-I/O	PD/PU in Soc	PD 15 KΩ ±5% on downstream facing port PU 1.5 KΩ ±5% on upstream facing port
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/PU in SoC	PD 15 KΩ ± 5% on downstream facing port PU 1.5 KΩ ±5% on upstream facing port
A46	USB0+				
A47	VCC_RTC	Real Time Clock (RTC) circuit power input	PWR 3V		Voltage range 2.8 V to 3.47 V
A48	EXCD0_PERST#	ExpressCard reset port 0	O-3.3	PD 10 kΩ	
A49	EXCD0_CPPE#	ExpressCard capable card request port 0	I-3.3	PU 10 kΩ, 3.3 V (S0)	
A50	LPC_SERIRQ	Serial interrupt request	I/OD-3.3	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 20 kΩ, 3.3 V (S0)	
A55	RSVD	Reserved for future use	NC		
A56	RSVD				
A57	GND	Power Ground	PWR GND		

Pin	COMe Signal	Description	Type	Termination	Description
A58	PCIE_TX3+	PCI Express transmit lane 3	DP-O		
A59	PCIE_TX3-				
A60	GND	Power Ground	PWR GND		
A61	PCIE_TX2+	PCI Express transmit lane 2	DP-O		
A62	PCIE_TX2-				
A63	GPI1	General purpose input 1	I-3.3	PU 20 kΩ, 3.3 V (S0)	
A64	PCIE_TX1+	PCI Express transmit lane 1	DP-O		
A65	PCIE_TX1-				
A66	GND	Power Ground	PWR GND		
A67	GPI2	General purpose input 2	I-3.3	PU 20 kΩ, 3.3 V (S0)	
A68	PCIE_TX0+	PCI Express transmit lane 0	DP-O		
A69	PCIE_TX0-				
A70	GND	Power Ground	PWR GND		
A71	LVDS_A0+	LVDS channel A DAT0 or EDP Lane 2 transmit	DP-O		
A72	LVDS_A0-				
A73	LVDS_A1+	LVDS channel A DAT1 or EDP Lane 1 transmit	DP-O		
A74	LVDS_A1-				
A75	LVDS_A2+	LVDS channel A DAT2 or EDP Lane 0 transmit	DP-O		
A76	LVDS_A2-				
A77	LVDS_VDD_EN	LVDS or EDP panel power control	O-3.3	PD 100 kΩ	
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
A82	LVDS_A_CK-				
A83	LVDS_I2C_CK	I2C Clock for LVDS display or eDP AUX +	I/O-3.3	PU 2.2 kΩ, 3.3 V (S0)	
A84	LVDS_I2C_DAT	I2C Data line for LVDS display or eDP AUX -	I/O-3.3	PU 2.2 kΩ, 3.3 V (S0)	
A85	GPI3	General purpose input 3	I-3.3	PU 20 kΩ 3.3V (S0)	
A86	RSVD	Reserved for future use	NC		
A87	eDP_HPD	Detection of Hot Plug / Unplug	I-3.3	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 20 kΩ	
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 10 kΩ	TMP does not use this functionality

Pin	COMe Signal	Description	Type	Termination	Description
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
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

5.5. Connector X1A Row B1 – B110

Table 30: 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#	Indicates the start of an LPC cycle	O-3.3		
B4	LPC_AD0	LPC multiplexed command, address and data bus	I/O-3.3		
B5	LPC_AD1				
B6	LPC_AD2				
B7	LPC_AD3				
B8	LPC_DRQ0#	LPC serial DMA master request	NC		Not supported on Apollo Lake SoC
B9	LPC_DRQ1#				
B10	LPC_CLK	LPC 25 MHz clock output	O-3.3	PD 20 kΩ in SoC	25 MHz
B11	GND	Power Ground	PWR GND		
B12	PWRBTN#	Power Button - a falling edge creates a power button event	I-3.3	PU 10 kΩ, 3.3 V	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.
B13	SMB_CLK	SMBus clock line	O-3.3	PU 2.56 kΩ, 3.3 V (S5)	
B14	SMB_DAT	SMBus bidirectional data line	I/O-3.3	PU 2.56 kΩ, 3.3 V (S5)	
B15	SMB_ALERT#	SMBus alert generates a SMI# or wakes the system	I/O-3.3	PU 2.2 kΩ, 3.3 V (S5)	
B16	SATA1_TX+	SATA transmit data pair 1	DP-O		
B17	SATA1_TX-				
B18	SUS_STAT#	Indicates imminent suspend operation; used to notify LPC devices.	O-3.3		
B19	SATA1_RX+	SATA receive data pair 1	DP-I		
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 61 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	NC		Not supported on Apollo Lake SoC
B29	HDA_SDIN1	Audio Codec serial data input 1	NC		
B30	HDA_SDIN0	Audio Codec serial data input 0	I-3.3		
B31	GND	Power Ground	PWR GND		

Pin	COMe Signal	Description	Type	Termination	Description
B32	SPKR	Speaker output provides the PC beep signal and is mainly intended for debugging purposes	O-3.3		
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	PU 2.21 kΩ, 3.3 V (S5)	
B35	THRM#	Input from off-module temp sensor indicating an over-temp situation	I-3.3	PU 10 kΩ, 3.3 V (S0)	No function implemented
B36	USB7-	USB 2.0 differential data pairs (host) port 7	DP-I/O	PD/PU in SoC	PD 15 kΩ +/- 5% on downstream facing port PU 1.5 kΩ +/- 5% on upstream facing port
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/PU in SoC	PD 15 kΩ +/- 5% on downstream facing port PU 1.5 kΩ +/- 5% on upstream facing port
B40	USB5+				
B41	GND	Power Ground	PWR GND		
B42	USB3-	USB 2.0 differential data pairs port 3	DP-I/O	PD/PU in SoC	PD 15 kΩ +/- 5% on downstream facing port PU 1.5 kΩ +/- 5% on upstream facing port
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/PU in SoC	PD 15 kΩ +/- 5% on downstream facing port PU 1.5 kΩ +/- 5% on upstream facing port
B46	USB1+				
B47	EXCD1_PERST#	ExpressCard expansion, reset port 1	O-3.3	PD 10 kΩ	
B48	EXCD1_CPPE#	ExpressCard expansion, capable card request port 1	I-3.3	PU 10 KΩ, 3.3 V (S0)	
B49	SYS_RESET#	Reset button input	I-3.3	PU 3.48 kΩ, 3.3 V (S5)	
B50	CB_RESET#	Carrier board reset- resets output from module to carrier board	O-3.3		
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 20 kΩ	
B55	RSVD	Reserved for future use	NC		
B56	RSVD				
B57	GPO2	General purpose output 2	O-3.3	PD 20 KΩ	
B58	PCIE_RX3+	PCI Express receive lane 3	DP-I		
B59	PCIE_RX3-				
B60	GND	Power Ground	PWR		

Pin	COMe Signal	Description	Type	Termination	Description
B61	PCIE_RX2+	PCI Express receive lane 2	DP-I		
B62	PCIE_RX2-				
B63	GPO3	General purpose output 3	O-3.3	PD 20 KΩ	
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 wake up signal, to implement wake-up on PS2 keyboard or mouse	I-3.3	PU 10 KΩ, 3.3 V (S5)	
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 on Apollo Lake SoC
B78	DDI0_PAIR4-				
B79	LVDS/BKLT_EN	LVDS or EDP panel backlight enable (ON)	O-3.3	PD 100 kΩ	
B80	GND	Power Ground	PWR GND		
B81	DDI0_PAIR3+	DDIO data pair 3	DP-O		
B82	DDI0_PAIR3-				
B83	LVDS/BKLT_CTRL	LVDS or EDP panel backlight brightness control	O-3.3		
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)	
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 on Apollo lake SoC
B92	DDI0_PAIR5-				
B93	DDI0_PAIR6+	DDIO data pair 6	NC		Not supported on Apollo lake SoC
B94	DDI0_PAIR6-				Optional connection to USB2_OTG_ID
B95	DDI0_DCC_AUX_SEL	DDIO DCC/ Aux select	I-3.3	PD 1 MΩ	
B96	USB_HOST_PRSNT	USB host preset	I-3.3	PD 100 kΩ	Internal connection to USB2_VBUS_SNS
B97	SPI_CS#	Chip select for carrier board SPI	O-3.3		
B98	DDI0_CTRLCLK_AUX+	DDIO auxiliary clock control signal	I/O-3.3 v	PD 100 kΩ	

Pin	COMe Signal	Description	Type	Termination	Description
B99	DDI0CTRLDATA_AUX-	DDI0 auxiliary data control signal		PU 100 kΩ, 3,3V (S0)	
B100	GND	Power Ground	PWR GND		
B101	FAN_PWMOUT	Fan speed control by PWM Output	O-3.3		20 V protection circuit implemented on module, PD on carrier board needed for proper operation. Default frequency of PWM signal is 25kHz.
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-m4AL10 uses a Kontron-customized, pre-installed and configured version of AMI EFI BIOS Aptio ® 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-m4AL10.

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

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

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

1. Power on the board.
2. Wait until the first characters appear on the screen (POST messages or splash screen).
3. Press the <DEL> key.
4. If the uEFI BIOS is password-protected, a request for password will appear. Enter either the User Password or the Supervisor Password (see Chapter 6.4.4: Security Setup Menu), press <RETURN>, and proceed with step 5.
5. A Setup menu appears.

6.2. Navigating the uEFI BIOS

The COMe-m4AL10 uEFI BIOS Setup program uses a hot key navigation system. The hot key legend bar is located at the bottom of the setup screens. The following table provides a list of navigation hot keys available in the legend bar.

Table 31: Navigation Hot Keys Available in the Legend Ba

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.

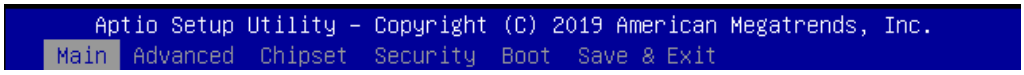
6.3. Getting Help

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 12: Setup menu Selection Bar



The Setup menus available for the COMe- m4AL10 are: :

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

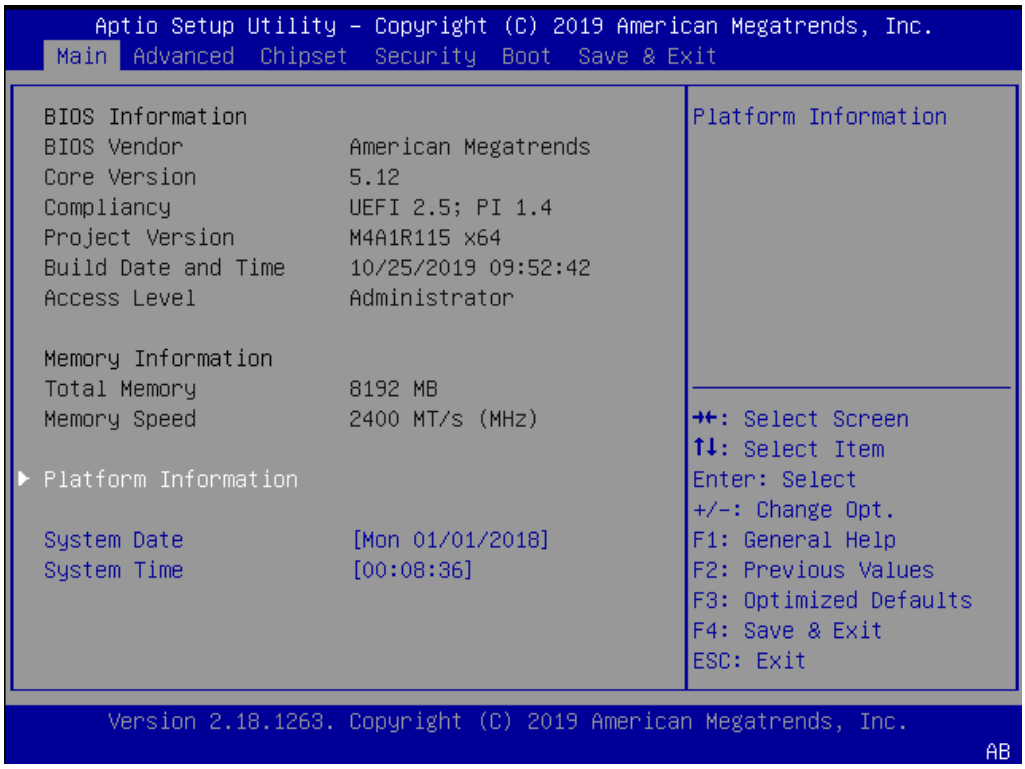
The currently active menu is highlighted in grey and the currently active uEFI BIOS setup item is highlighted in white. Use the left and right arrow keys to select the Setup menu.

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

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

Figure 13: Main Setup Menu Screen



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

Table 32: Main Setup Menu Sub-screens and Functions

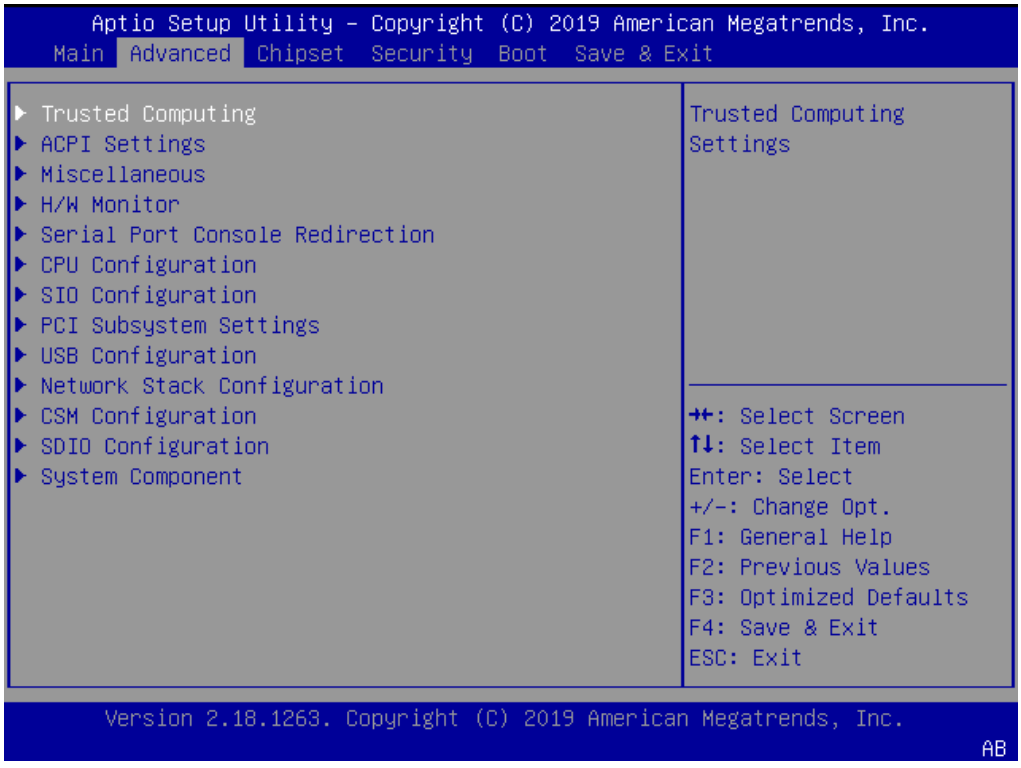
Sub-Screen	Description
BIOS Information>	Read only field BIOS vendor, Core version, Compliancy, Project version, Build date and time, and Access level
Memory Information>	Read only field Total memory and memory speed MT/s (MHz)
Platform Information>	Read only field *Module Information* Product name, Revision, Serial # ,MAC address, Boot counter, and CPLD rev
	Additional information for MAC Address The MAC address entry is the value used by the Ethernet controller and may contain the entry 'Inactive' - Ethernet chip is inactive. To activate the Ethernet chip set the following: Advanced > Network Stack Configuration > Network Stack > Enable 88:88:88:88:87:88 is a special pattern that will be filled in by the Ethernet firmware if there is no valid entry in the firmware block of the BIOS SPI (i.e. the MAC address has been overwritten during the last attempt to flash the system).
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 displays sub-screens and second level sub-screens with functions, for advanced configurations.

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

Figure 14: Advanced Setup Menu Screen



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

Table 33: Advanced Setup menu Sub-screens and Functions

Sub-Screen	Function	Second level Sub-Screen / Description
Trusted Computing>	Read only Information TPM20 device Found, Vendor and Firmware version	
	Security Device Support>	Enables or disables BIOS support for security device Operating System will not show security device, and TCG EFI protocol and INT1A interface are not available. [**Enabled**, Disabled]
	Active PCR Banks>	Read only field Displays active PCR Banks
	Available PCR Banks>	Read only field Displays available PCR Banks
	SHA-1 PCR Bank>	SHA-1 PCR Bank [**Enabled**, Disabled]
	SHA256 PCR Bank>	SHA256 PCR Bank [**Enabled**, Disabled]

Sub-Screen	Function	Second level Sub-Screen / Description	
Trusted Computing> (continued)	Pending Operation>	Schedules an operation for security device Note: Computer reboots on restart to change the state of the security device. [**None**, TPM Clear]	
	Platform Hierarchy>	Platform Hierarchy [**Enabled**, Disabled]	
	Storage Hierarchy>	Storage Hierarchy [**Enabled**, Disabled]	
	Endorsement Hierarchy>	Endorsement Hierarchy [**Enabled**, Disabled]	
	TPM2.0 UEFI Spec Version>	Selects TCG2 Spec Version support TCG_1_2: is compatible mode for Win8/Win10 and TCG_2: supports TCG2 protocol and event format Win 10 or later. [TCG_1_2, **TCG_2**]	
	Physical Presence Spec Version>	Select to inform OS to support either PPI Spec 1.2 or 1.3 Note: Some HCK tests might not support 1.3. [1.2, **1.3**]	
	TPM 20 InterfaceType>	Read only field	
	Device Select>	Selects BIOS support for security devices. Auto: supports both TPM 1.2 and TPM 2.0 TPM 1.2: restricts support to TPM 1.2 devices TPM 2.0: restricts support to TPM 2.0 devices [TPM 1.2, TPM 2.0, **Auto**]	
ACPI Settings>	Enable ACPI Auto Configuration>	Enables or disables BIOS ACPI auto configuration. If enabled, the system uses generic ACPI settings that may not fit the system best. [Enabled, **Disabled**]	
	Enable Hibernation>	Enables or disables systems ability to hibernate (OS/S4 Sleep State) This option may not be effective with some operating systems. [**Enabled**, Disabled]	
	ACPI Sleep State>	Selects highest ACPI sleep state the system enters when the SUSPEND button is pressed [Suspend Disabled, **S3 Suspend to Ram**]	
	Lock Legacy Resources>	Lock of legacy resources [Enabled, **Disabled**]	
Miscellaneous>	Watchdog>	Auto Reload>	Enables automatic reload of watchdog timers on timeout [Enabled, **Disabled**]
		Global Lock>	Enable sets all Watchdog registers (except for WD_KICK) to read only, until the module is reset. [Enabled, **Disabled**]
		Stage 1 Mode>	Selects action for Watchdog stage 1 [**Disable**, Reset, Delay, WDT Signal only]
	Additional Information two-staged watchdog Programmable stages to trigger different actions - If one stage is disabled, then the next stage is also disabled. Common actions for a watchdog trigger events 'Delay', 'Reset' and 'Watchdog signal only' CPLD code allows for triggering NMI or SCI. This requires programming of a predefined action inside the BIOS and therefore can only be used in a customized BIOS solution. Timeouts can be set to eight different fixed values between 1 second and 30 minutes.		

Sub-Screen	Function	Second level Sub-Screen / Description
Miscellaneous> (continued)	Reset Button Behavior>	Selects reset button behavior [**Chipset Reset**, Power Cycle]
	I2C Speed>	Selects internal I2C bus speed between (1 kHz and 400 kHz) For a default system 200 kHz is an appropriate value.
	On-board I2C Mode>	Keep 'Multimaster' setting unless otherwise noted [**MultiMaster**, BusClear]
	Manufacturing Mode>	Read only field Function is **disabled**
	LID Switch Mode>	Shows or hides Lid Switch Inside ACPI OS [Enabled, **Disabled**]
	Sleep Button Mode>	Shows or hides Sleep Button inside ACPI OS [Enabled, **Disabled**]
	SMBus device ACPI Mode	Hides the SMBus device from OS if set to hidden, otherwise device is visable [**Hidden**, Normal]
	CPLD device ACPI mode	Hides CPLD device from OS if set to hidden, otherwise device is visible [**Hidden**, Normal]
	SDIO/GPIO Output>	Output of SDIO/COMe-GPIO [**Enabled**, Disabled]
	SDIO/GPIO Mode>	Selects SDIO or COME-GPIO Mode [SDIO, **COME-GPIO**]
H/W Monitor>	CPU Temperature>	Read only field CPU temperature (°C) and Module temperature (°C)
	Module Temperature>	Read only field Module temperature (°C)
	CPU Fan – Fan Control>	Sets CPU Fan Control mode Disable - stops fan. Manual – manually sets the fan Auto – Hardware monitor controls cooling, similar to ACPI based 'Active Cooling', without producing a software load to the system. [Disabled, Manual, **Auto**]
	CPU Fan – Fan Pulse>	Displays number of pulses the fan produces during one revolution. (Range: 1-4)
	CPU Fan – Fan Trip Point>	Displays temperature at which the fan accelerates. (Range: 20°C – 80°)
	CPU Fan – Trip Point Speed>	Displays Fan speed at trip point in %. Minimum value is 30 %. Fan always runs at 100 % at (TJmax.-10°C).
	CPU Fan – Ref. Temperature>	Determines temperature source used for automatic fan control [**Module Temperature**, CPU Temperature]
	Additional Information CPU Temperature The CPU temperature value is taken from a NTC thermal resistor that is placed very close to the CPU. The NTC thermal resistor is not capable of measuring very fast rises and falls in temperature and measurements show a certain non-linearity. The NTC thermal resistor gives a general indication of the temperature close to the CPU. If the NTC thermal resistor value is compared to internal CPU values (i.e. DTS based values) certain differences are expected. These differences are due to the design and are not a bug. The NTC thermal resistor method was chosen because the CPU does not support PECI based temperature	

Sub-Screen	Function	Second level Sub-Screen / Description	
H/W Monitor> (continued)	measurement, and does not supply an internal diode on the CPU's die that can be used instead of PECI. Reading the DTS based values would harm the system's real-time behavior and is therefore not used.		
	External Fan-Fan Control>	Sets Fan Control mode for external fan Disable - stops the fan Manual – manually set the fan Auto - hardware monitor controls cooling, similar to ACPI based 'Active Cooling', without producing a software load to the system. [Disable, Manual, **Auto**]	
	External Fan–Fan Pulse>	Displays number of pulse the fan produces during one revolution (Range: 1-4)	
	External Fan-Fan Trip point>	Displays temperature at which fan accelerates. (Range: 20°C to 80°C)	
	External Fan-Trip Point Speed>	Displays fan speed at trip point in %. Minimum value is 30% Fan always runs at 100% at (TJmax.-10°C)	
	External Fan Reference Temperature>	Determines temperature source used for automatic fan control [**Module Temperature**, CPU Temperature]	
	Additional Information External Fan An external fan can be connected to baseboard. The external fan's control lines are routed via the COMe connector.		
	5.0V Standby>	Read only field Displays standby voltage	
	Batt Volt. at COMe pin>	Read only field Displays battery voltage at COMe pin	
	Widerange VCC>	Read only field Displays wide range VCC	
Serial Port Console Redirection>	COM0 Console Redirection>	Console redirection via COMe module's COM1 [Enabled, **Disabled**]	
	COM1 Console Redirection>	Console redirection via COMe module's COM2 [Enabled, **Disabled**]	
	COM2 Console Redirection>	Console redirection via COMe module's COM3 [Enabled, **Disabled**]	
	COM3 Console Redirection>	Console redirection via COMe module's COM4 [Enabled, **Disabled**]	
	Additional Information COM # Console If redirection is enabled then the port settings such as Terminal type, Bits per second, Data bits, Parity etc. can be adjusted here. On-module COM ports do not support flow control. If the Port is disabled, the COM# port is displayed as a read only field.		
	Legacy Console Redirection settings>	Legacy Serial Redirection Port>	Selects a COM port to display redirection of legacy OS and legacy OPROM messages [**COM0**, COM1, COM2, COM3]
	Serial Port for Out-of-Band Management / Windows EMS Console Redir.>	Console redirection [Enabled, **Disabled**]	

Sub-Screen	Function	Second level Sub-Screen / Description	
CPU Configuration>	Socket 0 CPU Information>	Read only field Processor Type, CPU signature, Microcode patch, Max. CPU Speed, Min. CPU speed, processor Cores, Intel HT technology, intel VT-x technology, L1 Data Cache, L1 Code Cache, L2 Cache and L3 Cache.	
	Read only field Speed and 64 bit		
	CPU Power Management Configuration>	EIST>	Intel Speedstep [**Enabled**, Disabled]
		Turbo Mode>	Enables or disables processor turbo mode Note: EMTTM must also be enabled. Auto means enabled unless the max. turbo ratio is bigger than 16-SKL A0 W/A. [**Enabled**, Disabled]
		Boot Performance Mode>	Selects the performance state the BIOS sets before OS handoff [**Max. Performance**, Max. Battery]
		C-States>	Enables or disables CPU power management to allow CPU to enter C-State [**Enabled**, Disabled]
		Enhanced C-States>	Enables or disables C1E. If enabled CPU switches to minimum speed when all cores enter C-state. [**Enabled,** Disabled]
		Max. Package C-States>	Controls the maximum package C-state that the processor supports [**PC2**, PC1, C0]
		Max. Core C-State>	Controls the maximum core C-state that the cores support. [**Fused value**, Core C10, Core C9, Core C8 ,Core C7, Core C6, Core C1, Unlimited]
		C-State Auto Demotion>	Configures C-state auto demotion [Disabled, **C1**]
		C-State Un-demotion>	Configures C-state un-demotion [Disabled, **C1**]
	Active Processor Core>	Number of cores to be enabled in each processor package [Enabled, **Disabled**]	
	Intel (VME) Virtual Technology>	Enables VMM to utilize additional hardware capabilities provided by Vanderpool Technology [**Enabled**, Disabled]	
	VT-D>	CPU VT-d [Enabled, **Disabled**]	
	Bidirectional PROCHOT>	If a processor thermal sensor trips (either core), PROCHOT# is driven. If bi-direction is enabled, external agents can drive PROCHOT# to throttle the processor. [**Enabled,** Disabled]	
	Thermal Monitor>	Thermal monitor [**Enabled**, Disabled]	
	Monitor MWait>	Monitor Mwait [Enabled, Disabled, **Auto**]	

Sub-Screen	Function	Second level Sub-Screen / Description	
CPU Configuration> (continued)	P-State Coordinator>	Changed P-State coordination type [**HW_ALL**, SW_ALL, SW_ANY]	
	DTS>	Digital thermal sensor [Enabled, **Disabled]**	
SIO Configuration>	Read only field AMI SIO driver version		
	Serial Port 0>	Use This Device>	Enables or disables the use of this logical device [**Enabled**, Disabled]
		Logical Device Settings: Current>	Read only field IO=3F8h; IRQ=4
		Logical Device Settings: Possible>	Allows the user to change the device's resource settings. New settings are reflected on the setup page after system restarts. [**Use Automatic Settings**, IO=3F8h; IRQ=4, IO=3F8h; IRQ=3,4,5,7,9,10,11,12 IO=2F8h; IRQ=3,4,5,7,9,10,11,12, IO=3E8h; IRQ=3,4,5,7,9,10,11,12, IO=2E8h; IRQ=3,4,5,7,9,10,11,12]
	Serial Port 1>	Use This Device>	Enables or disables the use of this logical device [**Enabled**, Disabled]
		Logical Device Settings: Current>	Read only field IO=2F8h; IRQ=3
		Logical device setting: Possible>	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=2F8h; IRQ=3, IO=3F8h; IRQ=3,4,5,7,9,10,11,12 IO=2F8h; IRQ=3,4,5,7,9,10,11,12, IO=3E8h; IRQ=3,4,5,7,9,10,11,12, IO=2E8h; IRQ=3,4,5,7,9,10,11,12]
	Additional Information SIO: Warning: Logical Devices state on the left side of the control reflects the current logical device state. Changes made during the setup session are shown after restarting the system. Disabling SIO logical devices may have unwanted effects. The SIO Configuration menu enables all available serial interfaces to be configured. The module-based serial interfaces always appear as COM1 and COM2. COM 1 and COM 2 can be treated as 16550-compatible legacy COM interfaces at the standard I/O addresses and are based in the on-module CPLD. Note: Hardware flow control is not supported. Optionally, If the baseboard contains an activated SuperIO of the type Winbond 83627, then its serial interfaces are added to the system as COM3 and COM4. COM3 and COM4 IRQ and I/O addresses are configurable in this menu, too. Although the chipset internal COMs are not supported due to technical constraints their driver must be installed. Installing the driver does not mean that these serial interfaces are useable.		

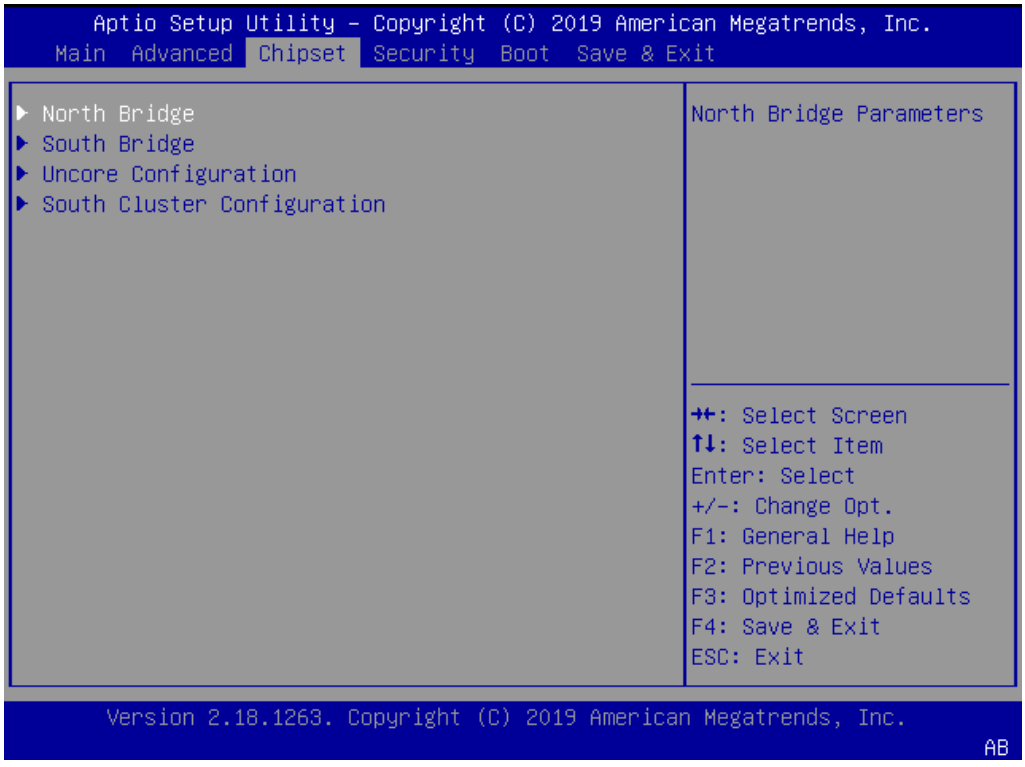
Sub-Screen	Function	Second level Sub-Screen / Description
Network Stack Configuration>	Network Stack>	UEFI network stack [Enabled, **Disabled**]
	Ipv4 PXE Support>	Enables Ipv4 PXE boot support Note: If disabled IPV4 PXE boot option is not created. [**Enabled**, Disabled]
	Ipv4 HTTP Support>	Enables Ipv4 HTTP boot support Note: If disabled IPV4 HTTP boot option is not created. [Enabled, **Disabled**]
	Ipv6 PXE Support>	Enabled Ipv6 PXE boot support Note: If disabled IPV6 PXE boot option is not created. [Enabled, **Disabled]**
	Ipv6 HTTP Support>	Enables Ipv6 HTTP boot support Note: If disabled IPV6 HTTP boot option is not created. [Enabled, **Disabled]**
	PXE Boot Wait Time>	Displays wait time to press ESC key to abort the PXE boot
	Media Detect Count>	Displays number of times presence of media is detected
USB Configuration>	Read only fields USB Configuration, UBS module Version, USB controllers, and USB devices	
	Legacy USB Support>	Enable- supports legacy USB Auto– disables legacy support, if no USB devices are connected Disable-keeps USB devices available for EFI applications only [**Enabled**, Disabled, Auto]
	XHCI Hand-off>	XHCI ownership change claimed by XHCI driver. Note: This is a work around for OS(s) without XHCI hand-off support. [**Enabled,** Disabled]
	USB Mass Storage Driver Support>	Enables or disables USB mass storage driver support [**Enabled,** Disabled]
	USB Transfer Time-out>	Displays timeout value for control, bulk and interrupt transfers [1 sec, 5 sec, 10 sec, **20 sec**]
	Device Reset Time-out>	Displays USB mass storage device start unit command time-out [10 sec, **20 sec**, 30 sec, 40 sec]
	Device Power-up Delay>	Displays maximum time taken for the device to report itself to the host properly. Auto uses the default :root port 100 ms /hub port delay is taken from hub port descriptor. [**Auto**, Manual]

6.4.3. Chipset Setup Menu

On entering the Chipset Setup menu, the screen lists four sub-screen options North bridge, South bridge, Uncore Configuration and South Cluster Configuration.

6.4.3.1. Chipset> North Bridge

Figure 15: Chipset > North Bridge Menu Screen



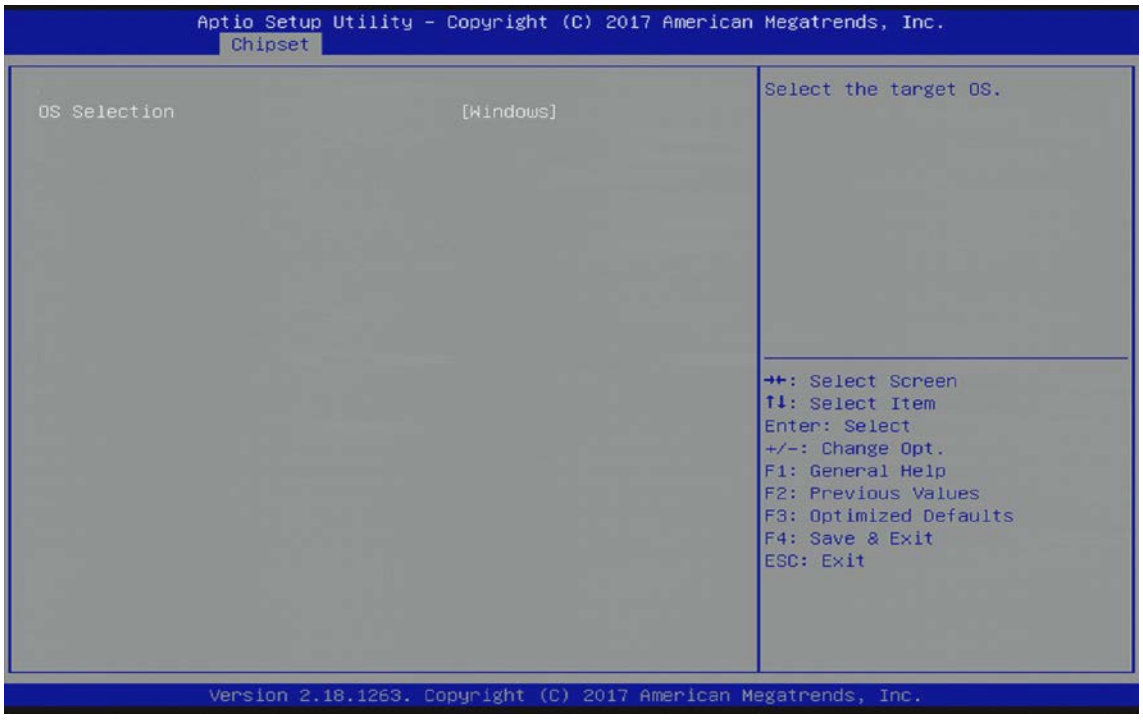
The following table shows the North bridge sub-screens and functions and describes the content. Default settings are in **bold**.

Table 34: Chipset Set > North Bridge Sub-screens and Function

Function	Second level Sub-Screen / Description	
Memory Configuration>	Read only field Total memory, MB (LPDDR4) / memory slot 0, MB (LPDDR4) / memory slot 1, MB (LPDDR4) / memory slot 2, MB (LPDDR4) / memory slot 3. MB (LPDDR4)	
	Max TOLUD>	Sets the maximum TOLUD value. Dynamic assignment adjustsTOLUD automatically, based on largest MMIO length of the installed graphic controller. [**2 GB**, 2.25 GB, 2.5 GB, 2,75 GB, 3 GB]
	Above 4GB MMIO BIOS Assignment>	Enables or disables above 4 GB memory mapped IO BIOS assignment. This is disabled automatically when aperture size is set to 2048 MB. [Enabled, **Disabled**]
	PCIE VGA Workaround>	Enable If PCIe card cannot boot in DOS. For test purposes only. [Enabled, **Disabled**]

6.4.3.2. Chipset > South Bridge

Figure 16: Chipset>South Bridge Menu Initial Screen



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

Table 35: Chipset Set> South Bridge Sub-screens and Functions

Function	Second level Sub-Screen / Description
OS Selection>	Selects target OS. [**Windows**, Android, Intel Linux]

6.4.4. Security Setup Menu

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

Figure 17: Security Setup Menu Screen

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

Table 36: Security Setup Menu Sub-screens and Functions

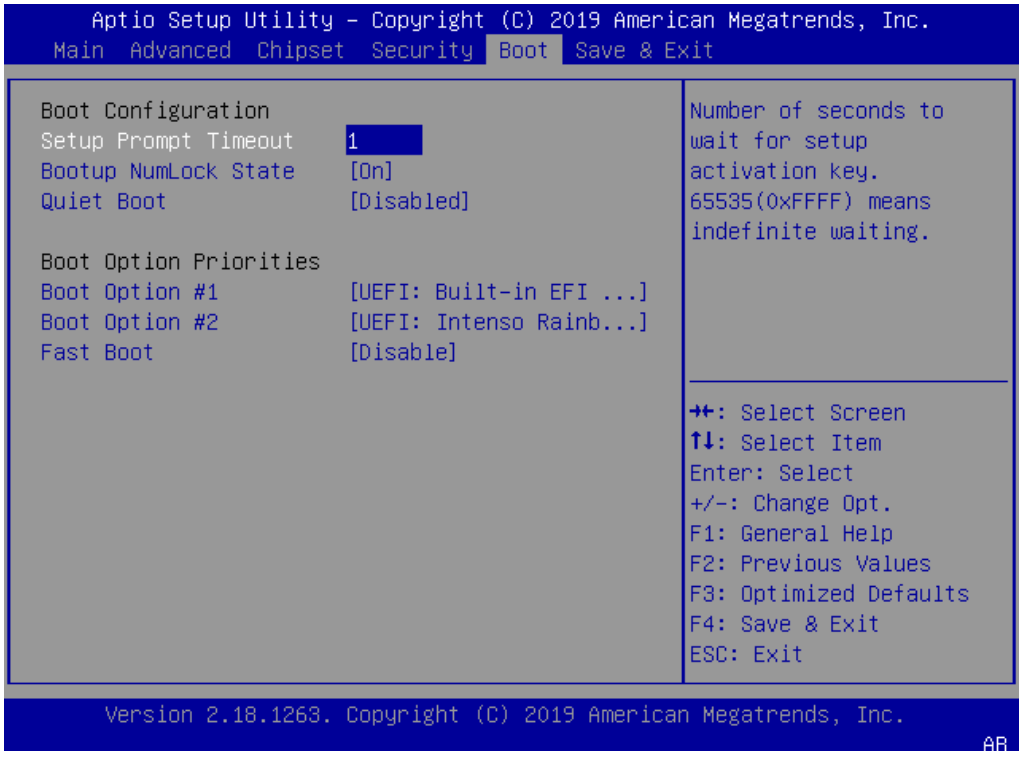
Function	Description
Setup Administrator Password>	Sets administrator password
User Password>	Sets user password
HDD Security Configuration>	Read Only Information Allows access to set, modify and clear Hard Disk user and master passwords. User Passwords need to be installed for Enabling Security. Master Password can be modified only when successfully unlocked with the Master Password in Post. If the 'Set HDD Password' is grayed out, then power cycle to enable the option again. HDD Password Configuration Security supported : Yes Security Enabled : No Security Locked : No Security Frozen : No HDD User Pwd Status : Not Installed HDD Master Pwd Status : Installed

Function	Description	
HDD Security Configuration> (continued)	Set User Password>	Sets HDD password. Note: It is advisable to power cycle the system after setting Hard Disk passwords. The 'Discarding or Saving Changes' in the setup does not have an impact on HDD when the password is set or removed. If the setup HDD user Password is grayed out, do power cycle enable the option again.

6.4.5. Boot Setup Menu

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

Figure 18: Boot Setup Menu Screen



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

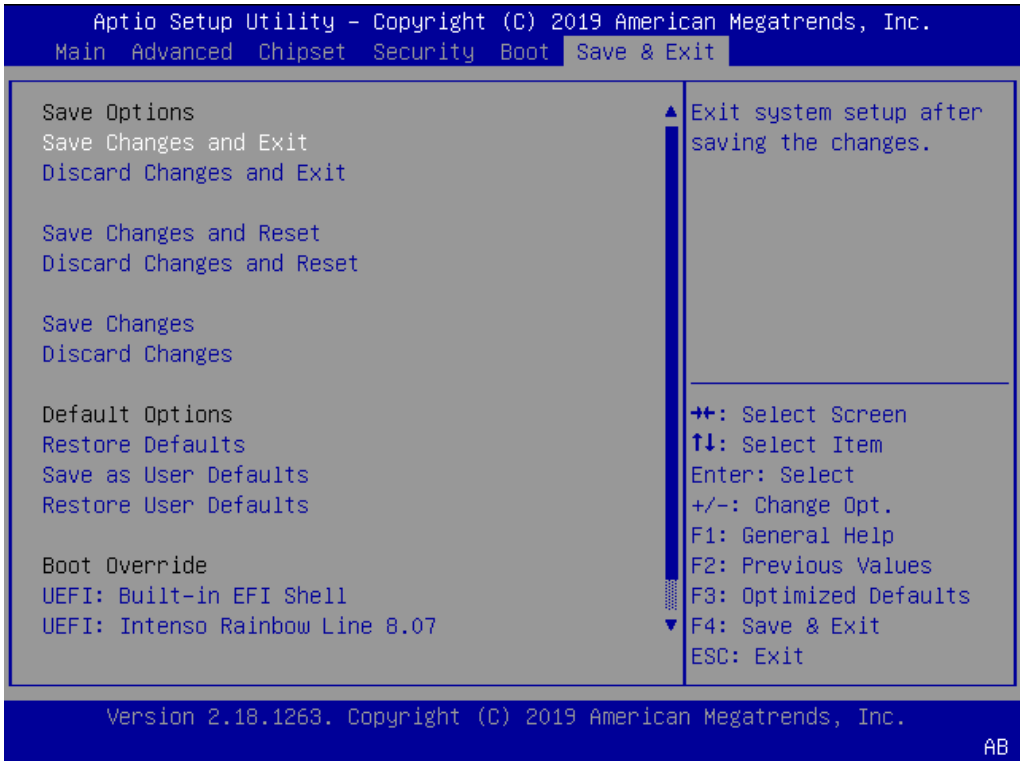
Table 37: Boot Setup Menu Sub-screens and Functions

Function	Description
Setup Prompt Timeout>	Displays number of seconds that the firmware waits for setup activation key The value 65535(0xFFFF) means an indefinite wait.
Bootup NumLock State>	Selects keyboard NumLock state [**ON**, OFF]
Quiet Boot>	Quiet Boot [Enabled, **Disabled**]
Boot Option #1>	Sets the system boot order [**UEFI: Built in EFI Shell**, Disabled]
Fast Boot>	Enables or disables FastBoot features Note: Most probes are skipped to reduce time and cost during boot. [Enabled, **Disabled**]

6.4.6. Save and Exit Setup Menu

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

Figure 19: Save and Exit Setup Menu Screen



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

Table 38: Save and Exit Setup Menu Sub-screens and Functions

Function	Description
Save Changes and Exit >	Exits system after saving changes
Discard Changes and Exit>	Exits system setup without saving changes
Save Changes and Reset>	Resets system after saving changes
Discard Changes and Reset>	Resets system setup without saving changes
Save Changes>	Saves changes made so far for any setup options
Discard Changes>	Discards changes made so far for any setup options
Restore Defaults>	Restores/loads standard default values for all setup options
Save as User Defaults>	Saves changes made so far as user defaults
Restore User Defaults>	Restores user defaults to all setup options
UEFI: IP4 Intel® I210 Gigabit Network Connection>	Attempts to launch the boot option #1
UEFI: KingstonDataTraveler 3.0PMAP, Partition 1>	Attempts to launch the boot option #2
UEFI: Built in EFI Shell>	Attempts to launch the boot option #3
Launch EFI Shell from File System Device>	Attempts to launch EFI Shell application (Shell.efi) from one of the available filesystem devices

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/).

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

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

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. It searches for scripts and executes them in the following order:

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

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 containing only the firmware images. The content of the archive with the directory structure must be copied onto a data storage device with FAT partition.

6.7.1. Firmware Updating Procedure

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

1. Copy the following files to an USB stick:

- flash.nsh (if available)
- fpt.efi
- fparts.txt
- m4AL10r<xxx>.bin (where xxx stands for the version #)

2. Start the system into uEFI BIOS setup (see Chapter 6.1 Starting the uEFI BIOS).
3. Disable the BIOS Lock.
4. Save and Exit the BIOS setup.
5. On the next start, boot into shell (see Chapter 6.5.1: Entering the uEFI Shell)
6. Change to the drive representing the USB stick.

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

7. Change to the directory where you copied the flash tool.

```
Cd <your_directory>
```

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

```
fpt  -F m4al10r<xxx>.bin
```

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

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

Changes made when the BIOS lock is disabled (previous step 3) are only effective during the first boot, after applying the changes. If the system is not flashed during the next, the update procedure might have to be repeated.

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.

Appendix A: List of Acronyms

Table 39: List of Acronyms

API	Application Programming Interface
BIOS	Basic Input Output System
BMC	Base Management Controller
BSP	Board Support Package
CAN	Controller-area network
Carrier Board	Application specific circuit board that accepts a COM Express ® module
COM	Computer-on-Module
COMe-b	COM Express® b=basic 125 mm x 95 mm module form factor
COMe-c	COM Express® c=compact 95 mm x 95 mm module form factor
COMe-m	COM Express® m=mini 84 mm x 55 mm module form factor
COP	Computer Operating Properly
CNTG	Computer Network Transaction Group
DDC	Display Data Control
DDC	Digital Down Converter
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
GPU-EU	Graphics Processing Unit- Execution Units
HBR2	High Bitrate 2
HDA	High Definition Audio (HD Audio)
HD/HDD	Hard Disk /Drive
HDMI	High Definition Multimedia Interface
HPM	PICMG Hardware Platform Management specification family
HWM	Hardware Monitor
IC	Integrated Circuit
I²C	Inter integrated Circuit Communications
I²S	Integrated Interchip Sound
IOL	IPMI-Over-LAN
IOT	Internet of Things
IPMI	Intelligent Platform Management Interface
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
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
OS	Operating System
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.
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
ShMC	Shelf Management Controller
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 Inteface
SSD	Solid State Drive
SSH	Secure Shell
TPM	Trusted Platform Module
UART	Universal Asynchronous Receiver Transmitter
UEFI	Unified Extensible Firmware Interface
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)

About Kontron – Member of the S&T Group

Kontron is a global leader in IoT/Embedded Computing Technology (ECT). As part of the S&T technology group, Kontron offers individual solutions in the areas of Internet of Things (IoT) and Industry 4.0 through a combined portfolio of hardware, software and services. With its standard and customized products based on highly reliable state-of-the-art technologies, Kontron provides secure and innovative applications for a wide variety of industries. As a result, customers benefit from accelerated time-to-market, lower total cost of ownership, extended product lifecycles and the best fully integrated applications.

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