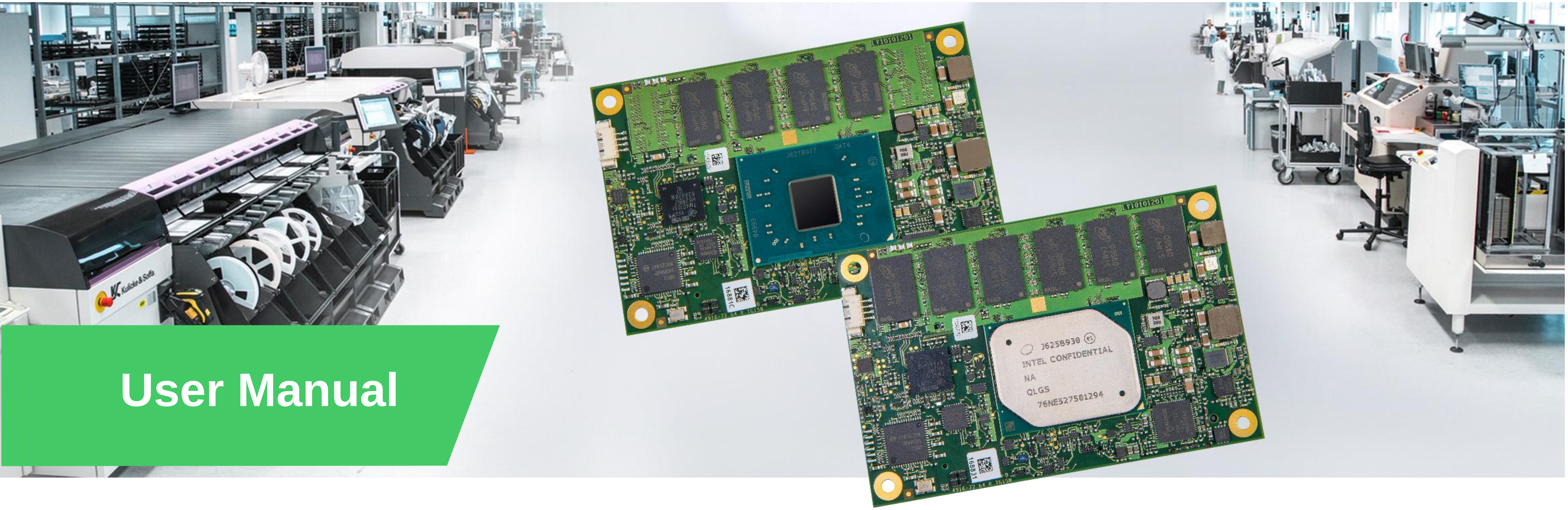
AVNET EMBEDDED



User Manual

COM Express® Mini Module

MSC C10M-AL

Type 10 Pinout

Intel® Atom™ / Celeron® / Pentium® Series SOC

Rev. 1.1 2022-05-17

Preface

Copyright Notice

Important Information

This documentation is intended for qualified audiences only. The product described herein is not an end user product. It was developed and manufactured for further processing by trained personnel.

Disclaimer

Although this document has been generated with the utmost care no warranty or liability for correctness or suitability for any particular purpose is implied. The information in this document is provided “as is” and is subject to change without notice.

EMC Rules

This unit must be installed in a shielded housing. If not installed in a properly shielded enclosure, and used in accordance with the instruction manual, this product may cause radio interference in which case the user may be required to take adequate measures at his or her owns expense.

Trademarks

All used product names, logos or trademarks are property of their respective owners.

Certification

Avnet Embedded GmbH is certified according to DIN EN ISO 9001:2015 standards.

Life-Cycle-Management

Avnet Embedded /MSC products are developed and manufactured according to high quality standards. Our life-cycle management assures long term availability through permanent product maintenance. Technically necessary changes and improvements are introduced if applicable. A product-change-notification and end-of-life management process assures early information of our customers.

Product Support

Avnet Embedded /MSC engineers and technicians are committed to provide support to our customers whenever needed.

Before contacting Avnet Embedded /MSC Technical Support, please consult the respective pages on our web site at embedded.avnet.com for the latest documentation, drivers and software downloads.

If the information provided there does not solve your problem, please contact us in Avnet Embedded /MSC Technical Support:

Phone:	+49 8165 906-200
E-Mail:	support.boards@avnet.eu

Contents

Revision History

Rev.	Date	Description
1.0	2021-03-08	First Release
1.1	2022-05-17	Added USB Overcurrent connection info. Adapted Corporate info.

Reference Documents

[1] COM Express Module Base Specification
COM Express Revision 2.1
Last update: April 10th, 2012

[2] PCI Local Bus Specification Rev. 2.1
PCI21.PDF
Last update: June 1st, 1995
http://www.pcisig.com

[3] ATA/ATAPI-6 Specification
d1410r3b.pdf
http://www.t13.org/

[4] Serial ATA Specification
Serial ATA 1.0 gold.pdf
Last update: August 29th, 2002 Rev.1.0
http://www.sata-io.org/

[5] IEEE Std. 802.3-2002
802.3-2002.pdf
http://www.ieee.org

[6] VESA Embedded DisplayPort Standard
eDP_v1_3 mem.pdf
Last update: 13.01.2012
http://www.vesa.org/

[7] Universal Bus Specification
usb_20.pdf
Last update: April 27th, 2000
http://www.usb.org

[8] Universal Serial Bus Revision 3.0 Specification
usb_30_spec_xxxxxx.zip
Last update: 13.08.2012
http://www.usb.org

1 User Information

1.1 About this Manual

This user’s guide provides information about the components, features and connectors available on the MSC C10M-AL COM Express® Mini Module.

1.2 Symbols and Signal Words

Safety Messages: Danger, Warning and Caution

No safety messages used in this manual, due to high compact module security. The following paragraph shows the usual MSC standard.

Signal words call attention to a safety message and designate a degree or level of hazard seriousness.

Signal word	Degree of hazard seriousness
Danger	Indicates a hazardous situation that, if not avoided, **will result in death or serious injury.**
Warning	Indicates a hazardous situation that, if not avoided, **could result in death or serious injury.**
Caution	Indicates a hazardous situation that, if not avoided, **could result in minor or moderate injury.**

All safety messages have a safety alert symbol and are structured as follows:

⚠ **Danger, Warning or Caution**

Type of hazard

Potential consequences of the hazard

Evasive or avoidance actions to be taken

Notice

Notices contain important information that should be observed. In case of neglect the board can be damaged. All notices have the ⓘ-symbol and are structured as follows:

ⓘ NOTICE: **Notice text.**

1.3 Table Cells with Gray Text

Cells with gray text contain information that is not supported on this board.

.

1.4 Intended Use

High-performance embedded modules can perform various tasks in infotainment systems, such as professional audio equipment for radio and television, or sophisticated illumination engineering for theater performances. The MSC C10M-AL module is based on Intel‘s multi-core system-on-chip (SOC) Atom generation that integrates next generation Intel processor core, graphics, memory, and I/O interfaces into one solution. Do not use this Mini Module in any other circumstances, as described herein.

1.5 Non-intended use

ⓘ NOTICE: **Use the compact module in the specified temperature ranges only!**

ⓘ NOTICE: **Use the compact module in the specified humidity ranges only!**

1.6 Electrostatic Sensitive Device

The MSC COM Express® Mini Module is an electrostatic sensitive device. It is packed accordingly.

ⓘ NOTICE: **Handle the Compact Module at electrostatic-free workstations only.**

ⓘ NOTICE: **Do not handle or store the Compact Module near strong electrostatic, electromagnetic, magnetic or radioactive fields unless the Compact Module is contained within its original packaging**

2 Technical Description

2.1 Introduction

COM Express® is an open specification from PICMG (PCI Industrial Computer Manufacturer Group). It is a module concept to bring PCI Express and other newer technologies like SATA, USB 3.0 and different display interfaces onto a COM (Computer On Module).

A COM Express® module is plugged onto an application-specific base board and offers a migration path to future CPU technologies as they become available. Utilizing different form factors, COM Express® can be used for deeply embedded solutions all the way up to high performance platforms.

The design of the MSC C10M-AL module supports the Intel® Atom-Series System-on-Chip (SOC) platform enabling the embedded application to provide high performance processing with an excellent visual experience, together with power efficiency.

For evaluation and design-in of the COM Express® modules MSC offers evaluation baseboards and development motherboards providing the interface infrastructure for the COM Express® module using PC type connectors for external access.

Currently four module sizes are defined in the COM Express® Specification 2.1: the Mini Module, the Compact Module, the Basic Module and the Extended Module. The main difference between them is the over-all physical size and the performance envelope supported.

All module sizes of the same type use the same connectors and pin-outs and utilize several common mounting hole positions. This level of compatibility permits a carrier board designed to accommodate an Extended Module to also support a Basic or Compact Module.

Up to 440 pins of connectivity are available between COM Express® modules and the Carrier Board. Legacy buses such as PCI, parallel ATA, LPC, HDA are supported as well as new high speed serial interconnects such as PCI Express, Serial ATA and Gigabit Ethernet.

To enhance interoperability between COM Express® modules and Carrier Boards, seven common signaling configurations (Pin-out Types) have been defined to ease system integration.

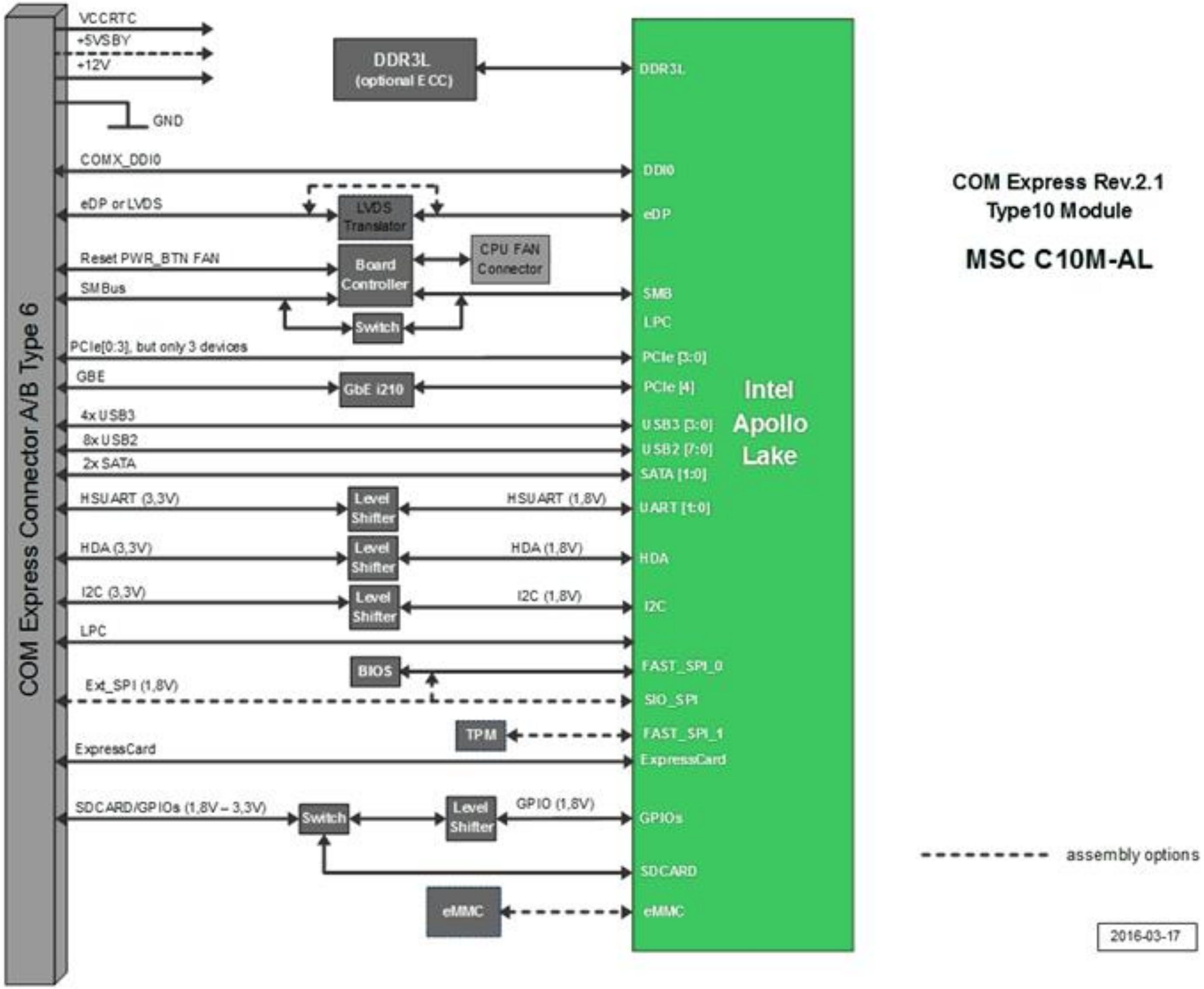
2.2 Key Features

The MSC C10M-AL COM Express® module is designed as a type 10 module according to COM Express® Module Base Specification Revision 2.1.

Key features include:

- Module size: 84 mm x 55 mm
- Intel® Atom™ / Celeron® / Pentium® Series System-on-Chip (SOC)
- Single 220 pin connector
- DDR3L on module up to 8 GB (optional ECC)
- Up to eight USB 2.0 ports; two can be used as USB 3.0 port; 4 shared over-current lines
- Two Serial ATA 6.0 Gbit/s ports
- Four PCI Express lanes for three devices
- Support pins for two Express Cards
- Display interfaces
  - two independent display controllers
  - Digital Display Interface (DDI) configurable as HDMI, DVI or Display Port
  - Single channel 24-bit LVDS channel (shared with eDP mounting option)
- High definition digital audio interface (external CODEC)
- Single GBit Ethernet interface (Intel® Ethernet Controller I210-AT or I210-IT)
- LPC interface
- Two high speed UART ports (TX and RX only, 16550 compliant)
- BIOS support for Super IO Winbond 83627 (on carrier board via LPC interface)
- Four GPI pins
- Four GPO pins
- +12V primary power supply input
- +5V standby (optional) and 3.3V RTC power supply inputs
- TPM module (optional TPM 2.0, SLB9670)
- Automatic fan control
- Watchdog timer
- Optional eMMC™ memory on module

2.3 Block Diagram



2.4 COM Express Implementation

COM Express® required and optional features for pin-out type 10 are summarized in the following table. The features identified as Minimum (Min.) **shall** be implemented by all modules. Features identified up to Maximum (Max) **may** be additionally implemented by a module.

The column MSC C10M-AL shows the features implemented by the MSC module.

		Type 10	MSC C10M-AL	Note
		Min / Max		
	System I/O			
A-B	PCI Express Lanes 0 - 3	1 / 4	4 (x1)	For three devices.
A-B	LVDS Channels	0 / 1	1	1x single channel, 1x24 Bit, Only available on modules with LVDS mounting option.
A-B	eDP on LVDS CH A pins	0 / 1	1	Only available on modules with eDP mounting option.
A-B	VGA Port	NA	0	
A-B	TV-Out	NA	0	
A-B	DDI 0	0 / 1	1	
A-B	Serial Ports 1- 2	0 / 2	2	HSUART
A-B	CAN interface on SER1	0 / 1	0	
A-B	SATA Ports	1 / 2	2	SATA 6.0 GBit/s
A-B	HDA Digital Interface	0 / 1	1	
A-B	USB 2.0 Ports	4 / 8	8	
A-B	USB Client	0 / 1	1	USB Port 7
A-B	USB 3.0 Ports	0 / 2	2	
A-B	LAN Port 0	1 / 1	1	Intel® Ethernet Controller I210-AT or Intel® Ethernet Controller I210-IT
A-B	Express Card Support	1 / 2	1	
A-B	LPC Bus	1 / 1	1	
A-B	SPI	1 / 2	1	
	System Management			
A-B	SDIO (muxed on GPIO)	0 / 1	1	Max. UHS-I
A-B	General Purpose Inputs	4 / 4	4	
A-B	General Purpose Outputs	4 / 4	4	
A-B	SMBus	1 / 1	1	
A-B	I^{2}C	1 / 1	1	
A-B	Watchdog Timer	0 / 1	1	

A-B	Speaker Out	1 / 1	1	
A-B	External BIOS ROM support	0 / 2	1	
A-B	Reset Functions	1 / 1	1	
	Power Management			
A-B	Thermal Protection	0 / 1	0	
A-B	Battery Low Alarm	0 / 1	1	
A-B	Suspend	0 / 1	1	
A-B	Wake	0 / 2	2	
A-B	Power Button Support	1 / 1	1	
A-B	Power Good	1 / 1	1	
A-B	VCC_5V_SBY Contacts	4 / 4	4	
A-B	Sleep Input	0 / 1	1	
A-B	Lid Input	0 / 1	1	
A-B	Fan Control Signals	0 / 2	2	
A-B	Trusted Platform Modules	0 / 1	1	optional TPM 2.0 module

2.5 Functional Units

CPUs (FCBGA 1296 package)	Intel® Atom^{TM} x5-E3930, DC, 1.30GHz, 1.80GHz Burst, 2 MB L2 Cache, 6.5W, 2ch DDR3L. (APL-I) Intel® Atom^{TM} x5-E3940, QC, 1.60GHz, 1.80GHz Burst, 2 MB L2 Cache, 9.5W, 2ch DDR3L. (APL-I) Intel® Atom^{TM} x7-E3950, QC, 1.60GHz, 2.00GHz Burst, 2 MB L2 Cache, 12W, 2ch DDR3L. (APL-I) Intel® Pentium^{TM} N4200, QC, 1.10GHz, 2.50GHz Burst, 2 MB L2 Cache, 6W, 2ch DDR3L Intel® Celeron^{TM} N3350, DC, 1.10GHz, 2.40GHz Burst, 2 MB L2 Cache, 6W, 2ch DDR3L. E3930, E3940, E3950: $T_{JUNCTION}$ = - 40°C to 110°C (APL-I, integrated heat spreader) N3350, N4200: $T_{JUNCTION}$ =0°C to 105°C
Memory	DDR3L on module for up to 8GB non-ECC unbuffered. (optional: ECC at Atom^{TM} x CPUs and DDR3L-1600) PC3-12800 DDR3L SDRAM (DDR3L-1600), PC3-14900 DDR3L SDRAM (DDR3L-1866).
SATA	2 SATA channels up to 6.0 GBit/s
USB	8 x USB 2.0, 2 x USB 3.0/2.0
USB Client	1 x USB 2.0 client
COM Express®	Type 10 interface, fully compliant to COM Express Base Specification R2.1
PCI Express™	Four channels PCIe x1. (For three devices)
LPC	Low Pin Count Bus for heritage interfaces
SPI	Serial Peripheral Interface for one 1.8 V SPI flash device
Graphics Controller	Integrated Intel® HD Graphics 505 with Atom^{TM} x7 and Pentium® CPU Integrated Intel® HD Graphics 500 with Atom^{TM} x5 and Celeron® CPUs
LVDS	Single channel 24-bit LVDS (Only available on modules with LVDS mounting option.)
Digital Display Ports	Two Digital Display Interfaces (DDI) (One is shared with LVDS) DP (4096x2304@60Hz) HDMI (3840x2160@30Hz) eDP (3840x2160@60Hz)
Ethernet	10/100/1000Base-TX (Intel® Ethernet Controller I210-AT for commercial temperature or Intel® Ethernet Controller I210-IT for industrial temperature)
Sound Interface	High Definition Audio Interface
Serial Interface	Two High Speed UARTs

Watchdog Timer	Embedded controller creates watchdog alert and system reset
TPM (option)	Optional TPM module, TPM 2.0, SLB9670
Fan Supply	4-pin header for support of a 12V PWM fan
Real Time Clock	RTC integrated in Intel® Atom SOC
CMOS Battery	External
System Monitoring	Voltages, temperatures, fan ▪ Core voltage ▪ 3.3V onboard voltage ▪ 12V input voltage ▪ 5V SBY input voltage ▪ CPU temperature (0°C - 100°C) ▪ System memory temperature ▪ Board temperature ▪ Fan speed and automatic fan speed control
SSD	Optional on module eMMC SSD

2.6 Power Supply

- **+12V primary power supply input**
- **+5V standby**
  Option, is not required for module operation.
  If not present, customer must ensure that the supply voltages which are generated on the carrier board are switched off during suspend states, so that no current from the carrier board's signal lines can flow to the CPU board.
- **3.3V RTC power supply**
  Option, is not required for module operation.
  BIOS SETUP data is stored in a nonvolatile backup memory device, therefore configuration data will not get lost after power removal (except for time and date information)

Voltage	Input range	Power Consumption
+12V	+4.75V - 20 V	Refer to chapter 2.7
+5V Standby	+4.75V - 5.25 V	
+3V RTC power supply	+2.5V - 3.47V	Typ. 4.3 µA

2.7 Power Dissipation

2.7.1 Running Mode

All measurements were made by plugging the MSC C10M-AL module onto a MSC C10-MB-EVA carrier. The module was equipped with various memory quantities. The table below shows typical values which refer to consumption of the module itself without consumption of the base board and CPU fan.

The following applications have been tested with minimum 15 minutes measurement time:

- Windows desktop (idle) under Microsoft Windows 10 64-bit.
- Running Intel® Thermal Analysis Tool (TAT!) Ver. 6.x to achieve TDP workload under Microsoft Windows 10 64-bit.
- BurnInTest V7.1 Pro with test settings 100% CPU, 100% RAM, 100% 2D Graphics and 100% 3D Graphics.

Module / CPU	Win 10 Idle	Win 10 TAT!		BurnInTest
		average	peak	
C10M-AL-E3930-240201I (Intel® Atom™ x5-E3930, 2C, 1.30GHz, 1.80GHz, 2MiB L2 Cache, 6.5W) 4GB non ECC	2.5 W	10.3 W	12.0 W	5.7 W
C10M-AL-E3940- 240201I (Intel® Atom™ x5- E3940, 4C, 1.60GHz, 1.80GHz, 2MiB L2 Cache, 9.5W) 4GB non ECC	2.5 W	14.1 W	14.7 W	7.5 W
C10M-AL-E3950- 351101I (Intel® Atom™ x7-E3950, 4C, 1.60GHz, 2.00GHz, 2MiB L2 Cache, 12W) 8GB ECC	2.8 W	20.6 W	25.2 W	9.7 W
C10M-AL-N4200- 350201C (Intel® Pentium™ N4200, 4C, 1.10GHz, 2.50GHz, 2MiB L2 Cache, 6W) 8GB non ECC	2.6 W	10.0 W[1)]	25.2 W[1)]	10.2 W

[1)] TAT workload setting: CPU-All 100%, Gfx 80% in Intel® Thermal Analysis Tool Ver. 6.0.1030, because TAT do not offer TDP for this SKU.

2.7.2 Power Dissipation (Standby Modes)

1. System is shut down into “Suspend to RAM” (S3) by Windows 10 64-bit with Wake on LAN enabled.
2. System is shut down into “Soft Off” (S5) or “Suspend to Disk” (S4) by Windows 10 64-bit with Wake on LAN enabled.

Module / CPU	Input Power	S3	S4 / S5
C10M-AL-E3930-240201I (Intel® Atom™ x5-E3930, 2C, 1.30GHz, 1.80GHz, 2MiB L2 Cache, 6.5W) 4GB non ECC	5V_SBY	0.45 W	0.32 W
C10M-AL-E3940- 240201I (Intel® Atom™ x5- E3940, 4C, 1.60GHz, 1.80GHz, 2MiB L2 Cache, 9.5W) 4GB non ECC	5V_SBY	0.36 W	0.23 W
C10M-AL-E3950- 351101I (Intel® Atom™ x7-E3950, 4C, 1.60GHz, 2.00GHz, 2MiB L2 Cache, 12W) 8GB ECC	5V_SBY	0.52 W	0.33 W
C10M-AL-N4200- 350201C (Intel® Pentium™ N4200, 4C, 1.10GHz, 2.50GHz, 2MiB L2 Cache, 6W) 8GB non ECC	5V_SBY	0.59 W	0.29 W

2.8 System Memory

The MSC C10M-AL CPU module provides on board memory which have to meet the following demands:

- non-ECC DDR3L and ECC DDR3L
- 1.35V Supply Voltage
- DDR3L-1600 / PC3-12800, DDR3L-1866 / PC3-14900 (ECC DDR3L only with DDR3L-1600)
- SPD (Serial Presence Detect) EEPROM.
- At temperatures above +60°C the memory refresh rate must be doubled with BIOS option *DDR double Refresh Rate* set to *Enabled*.

2.9 eMMC

When using the on-module eMMC storage device, it should be taken into consideration that the lifetime of the device is affected by the number of read/write and erase cycles. It is not recommended to use eMMC storage devices with applications which are continually storing large amounts of data.

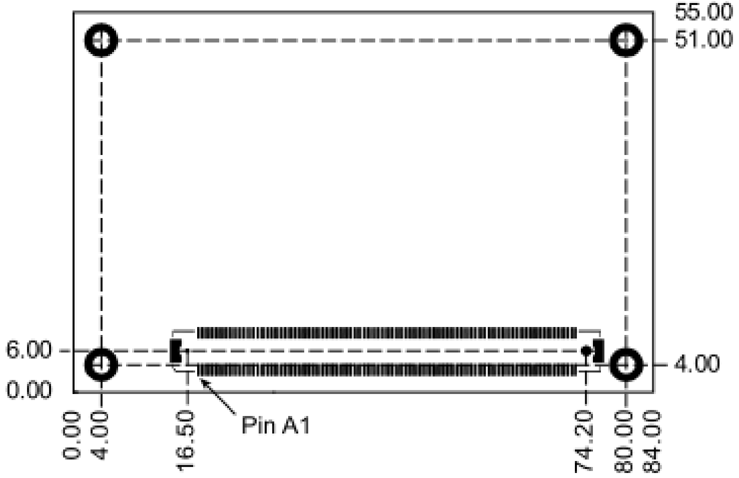
The eMMC device uses MLC (Multi Level Cell) technology.

Temperature Grade	Technology	Memory Size	Chip Identification
Extended (-25°C to +85°C)	MLC	16 GByte	Micron MTFC16GAKAECN-2M WT SanDisk SDINBDG4-16G-I1
Extended (-25°C to +85°C)	MLC	32 GByte	Micron MTFC32GAKAECN-3M WT SanDisk SDINBDG4-32G-I1
Industrial (-40°C to +85°C)	MLC	16 GByte	Micron MTFC16GAKAECN-4M IT SanDisk SDINBDG4-16G-XI1
Industrial (-40°C to +85°C)	MLC	32 GByte	Micron MTFC32GAKAECN-4M IT SanDisk SDINBDG4-32G-XI1

ⓘ NOTICE: With Windows 7 eMMC is not supported.

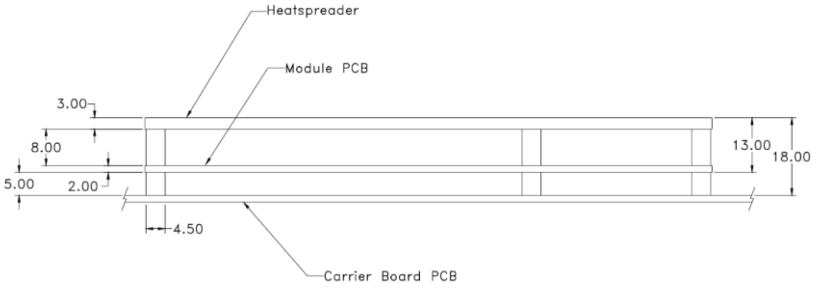
2.10 Mechanical Dimensions

2.10.1 Mini Module



There are two height options defined in the COM Express specification: 5mm and 8mm.

The height option is defined by the connectors on the baseboard.



The modules with Atom^{TM} APL-I CPUs are equipped with an integrated heat spreader. This heat spreader adds 1.00 mm to CPU height against modules with CPUs without integrated heat spreader. This has no effect to the z-height of a module with mounted spreader.

2.11 Thermal Specifications

The cooling solution of a COM Express module is based on a heat-spreader concept.

A heat-spreader is a metal plate (typically aluminum) mounted on the top of the module. The connection between this plate and the module components is typically done by thermal interface materials like phase change foils, gap pads and copper or aluminum blocks. A very good thermal conductivity is required in order to conduct the heat from the CPU and the chipset to the heat-spreader plate.

The heat-spreader of the MSC module is thermally attached using phase change materials and small aluminum blocks filling the gap between CPU and chipset dies and the heat-spreader plate.

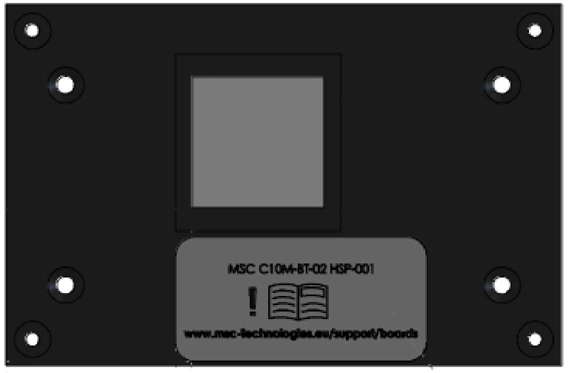
The heat-spreader is not a heat-sink! It is a defined thermal interface for the system designer with fixed mechanical dimensions, so it should be possible to interchange different module types without problems. There must be a cooling solution for the system. The surface temperature of the heat-spreader should not exceed 80°C.

Main issue for the thermal functionality of a system is that each device of the module is operated within its specified thermal values. The max value for the SOC is 105°C (T die). So there may be system implementations where the heat-spreader temperature could be higher.

Anyway, in this case it has to be validated that there are no thermal specification violations of any assembled part or integrated circuit over the system temperature range even at worst case conditions.

Environment:

Ambient Temperature:	0°C … 60°C (operating) -40°C … +85°C (operating, extended temp.) -25°C … +85°C (storage)
Humidity:	5 ... 95% (operating, non-condensing) 5 ... 95% (storage, non-condensing)



Additionally MSC offers adequate heat-sink solutions for the different COM Express modules depending on the power dissipation of the implemented CPU. For more information please refer to www.msc-technologies.eu or contact your sales representative.

2.12 Use Conditions

The Use Conditions define run-time parameters such as the operating mode (eg. 24/7), activity factor, max frequency, temperature range etc. for the target application.

Certain Use Conditions may have an effect on the lifetime of the product.

For industrial use cases where longer lifetime and higher activity factors may be required, processor manufacturers may recommend to limit the performance of the processing units.

For such purposes MSC provides a special BIOS version for extended reliability. This BIOS is available for download from our support website.

Please consult the relevant processor manufacturer datasheets for more information.

2.13 Signal Description

Pins are marked in the following tables with the power rail associated with the pin, and, for input and I/O pins, with the input voltage tolerance. The pin power rail and the pin input voltage tolerance **may** be different. For example, the PCI group is defined as having a 3.3V power rail, meaning that the output signals will only be driven to 3.3V, but the pins are tolerant of 5V signals.

An additional label, “Sus”, indicates that the pin is active during suspend states (S3, S4, S5). If suspend modes are used, then care must be taken to avoid loading signals that are active during suspend to avoid excessive suspend mode current draw.

Pin-Types:

I = Input.

O = Output.

OD = Open Drain output.

I/OD = Bi-directional Input/Open Drain Output Pin.

I/O = Bi-directional Input/Output.

ePU = external pull-up resistor on COM Express module.

ePD = external pull-down resistor on COM Express module.

eSR = external series resistor on COM Express module.

iPU = integrated pull-up resistor inside PCH or other IC, real value may vary from nominal one.

iPD = integrated pull-down resistor inside PCH or other IC, real value may vary from nominal one.

2.13.1 High Definition Audio

Signal	Pin Type	Signal Level	Power Rail	Remark / Tolerance	PU/PD/SR	Description	Source / Target
HDA_RST#	O	CMOS	3.3V Sus		eSR = 33 Ω	Reset output to CODEC, active low.	AL SOC
HDA_SYNC	O	CMOS	3.3V Sus		eSR = 33 Ω	48kHz fixed-rate, sample-synchronization signal to the CODEC(s),	AL SOC
HDA_BITCLK	O	CMOS	3.3V Sus		eSR = 33 Ω	24.00 MHz serial data clock generated by the FCH	AL SOC
HDA_SDOUT	O	CMOS	3.3V Sus		eSR = 33 Ω	Serial TDM data output to the CODEC, functional strap option	AL SOC
HDA_SDIN0	I	CMOS	3.3V Sus	3.3V	ePD = 100 KΩ	Serial TDM data inputs from up to 3 CODECs.	AL SOC

2.13.2 Ethernet

Signal	Pin Type	Signal Level	Power Rail	Remark / Tolerance	PU/PD/SR	Description	Source / Target
GBE0_MDI[0:3]+ GBE0_MDI[0:3]-	I/O	Analog	3.3V Sus	3.3V		Gigabit Ethernet Controller 0: Media Dependent Interface Differential Pairs 0,1,2,3. The MDI can operate in 1000, 100 and 10 Mbit / sec modes. MDI[0]+/- B1_DA+/- MDI[1]+/- B1_DB+/- MDI[2]+/- B1_DC+/- MDI[3]+/- B1_DD+/-	Intel® I210-AT/IT
GBE0_ACT#	OD	CMOS	3.3V Sus	5V / 20 mA		Gigabit Ethernet Controller 0 activity indicator, active low.	Intel® I210-AT/IT
GBE0_LINK#	OD	CMOS	3.3V Sus	5V / 20 mA		Gigabit Ethernet Controller 0 link indicator, active low.	Intel® I210-AT/IT
GBE0_LINK100#	OD	CMOS	3.3V Sus	5V / 20 mA		Gigabit Ethernet Controller 0 100 Mbit / sec link indicator, active low.	Intel® I210-AT/IT
GBE0_LINK1000#	OD	CMOS	3.3V Sus	5V / 20 mA		Gigabit Ethernet Controller 0 1000 Mbit / sec link indicator, active low.	Intel® I210-AT/IT
GBE0_CTREF	REF					N/A. Center tab voltage not needed by Intel® I210-AT/IT.	

2.13.3 Serial ATA

Signal	Pin Type	Signal Level	Power Rail	Remark / Tolerance	PU/PD/SR	Description	Source / Target
SATA0_TX+ SATA0_TX-	O	SATA	1.24V	AC coupled on module		Serial ATA Channel 0 transmit differential pair	AL SOC
SATA0_RX+ SATA0_RX-	I	SATA	1.24V	AC coupled on module		Serial ATA Channel 0 receive differential pair	AL SOC
SATA1_TX+ SATA1_TX-	O	SATA	1.24V	AC coupled on module		Serial ATA Channel 1 transmit differential pair	AL SOC
SATA1_RX+ SATA1_RX-	I	SATA	1.24V	AC coupled on module		Serial ATA Channel 1 receive differential pair	AL SOC
ATA_ACT#	OD	CMOS	3.3V	5V / 4mA		SATA activity indicator, active low	AL SOC

2.13.4 PCI Express Lanes

Signal	Pin Type	Signal Level	Power Rail	Remark / Tolerance	PU/PD/SR	Description	Source / Target
PCIE_TX[0:3]+ PCIE_TX[0:3]-	O	PCIe	1.24V	AC coupled on module		PCI Express Differential Transmit Pairs 0 through 3	AL SOC
PCIE_RX[0:3]+ PCIE_RX[0:3]-	I	PCIe	1.24V	AC coupled off module		PCI Express Differential Receive Pairs 0 through 3	AL SOC
PCIE_CLK_REF+ PCIE_CLK_REF-	O	PCIe CLK	1.05V			Differential Reference Clock output for all PCI Express and PCI Express Graphics lanes.	AL SOC

ⓘ NOTICE: Considerable care must be taken when using high speed signals on the carrier board. Reliable functionality depends on the following factors:

a. Trace length on the carrier board
b. Number of vias used on the carrier board
c. PCB material and specification used for the carrier board
d. Target device

2.13.5 Express Card Support

Signal	Pin Type	Signal Level	Power Rail	Remark / Tolerance	PU/PD	Description	Source / Target
EXCD[0]_CPPE#	I	CMOS	3.3V	3.3V	ePU = 10 KΩ	ExpressCard card request, active low	AL SOC
EXCD[1]_CPPE#	I	CMOS	3.3V	3.3V	ePU = 10 KΩ	ExpressCard card request, active low	AL SOC
EXCD[0]_RST#	O	CMOS	3.3V	3.3V	ePU = 10 KΩ	ExpressCard reset, active low	AL SOC
EXCD[1]_RST#	O	CMOS	3.3V	3.3V	ePU = 10 KΩ	ExpressCard reset, active low	AL SOC

2.13.6 USB

Attention: For USB Overcurrent Detection specifics, see Note 1 on next page!

Signal	Pin Type	Signal Level	Power Rail	Remark / Tolerance	PU/PD/SR	Description	Source / Target
USB[0:7]+ USB[0:7]-	I/O	USB	3.3V Sus	3.3V	iPD = 15 KΩ iSR = 45 Ω	USB differential pairs, channels 0 through 7	AL SOC
USB_HOST_PRSNT	I	CMOS	3.3V Sus	3.3V	ePD = 100 KΩ	A high value indicates that a host is present at USB7 port.	AL SOC
USB_0_1_OC#	I	CMOS	3.3V Sus	3.3V	ePU = 10 KΩ	USB over-current sense, USB channels 0 and 1. Pull-up is present on the module - do NOT pull this line high on the Carrier Board! Pull this line LOW only by an Open-Drain driver on the Carrier Board. **ATTENTION: SEE NOTE 1 BELOW!**	AL SOC
USB_2_3_OC#	I	CMOS	3.3V Sus	3.3V	ePU = 10 KΩ	USB over-current sense, USB channels 2 and 3. Pull-up is present on the module - do NOT pull this line high on the Carrier Board! Pull this line LOW only by an Open-Drain driver on the Carrier Board. **ATTENTION: SEE NOTE 1 BELOW!**	AL SOC
USB_4_5_OC#	I	CMOS	3.3V Sus	3.3V	ePU = 10 KΩ	USB over-current sense, USB channels 4 and 5. Pull-up is present on the module - do NOT pull this line high on the Carrier Board! Pull this line LOW only by an Open-Drain driver on the Carrier Board. **ATTENTION: SEE NOTE 1 BELOW!**	AL SOC
USB_6_7_OC#	I	CMOS	3.3V Sus	3.3V	ePU = 10 KΩ	USB over-current sense, USB channels 6 and 7. Pull-up is present on the module - do NOT pull this line high on the Carrier Board! Pull this line LOW only by an Open-Drain driver on the Carrier Board. **ATTENTION: SEE NOTE 1 BELOW!**	AL SOC
USB_SSTX[0:1]+ USB_SSTX[0:1]-	O	USB 3.0	1.24V Sus	AC coupled on module		USB 3.0 Differential Transmit Pairs 0 through 1	AL SOC
USB_SSRX[0:1]+ USB_SSRX[0:1]-	I	USB 3.0	1.24V Sus	AC coupled off module		USB 3.0 Differential Receive Pairs 0 through 1	AL SOC

NOTE 1:

The Apollo Lake chipset offers only 2 Overcurrent Detection lines in total. Thus the 4 lines that the COM Express standard offers need to be combined logically into these only two Overcurrent signals.

- **USB_0_1_OC# and USB_2_3_OC#** are electrically separate (not just shorted together), but **logically OR'ed together.**
- **USB_4_5_OC# and USB_6_7_OC#** are electrically separate (not just shorted together), but **logically OR'ed together.**

If an Overcurrent condition occurs on **either one** of USB0, USB1, USB2 or USB3, **all of USB0...USB3** will be deactivated simultaneously.

If an Overcurrent condition occurs on **either one** of USB4, USB5, USB6 or USB7, **all of USB4...USB7** will be deactivated simultaneously.

As stated above, this limitation is forced by the chipset and cannot be changed.

ⓘ NOTICE: Considerable care must be taken when using high speed signals on the carrier board. Reliable functionality depends on the following factors:

a. Trace length on the carrier board
b. Number of vias used on the carrier board
c. PCB material and specification used for the carrier board
d. Target device

2.13.7 LPC Bus

Signal	Pin Type	Signal Level	Power Rail	Remark / Tolerance	PU/PD/SR	Description	Source / Target
LPC_AD[0:3]	I/O	CMOS	3.3V	3.3V		LPC multiplexed address, command and data bus	AL SOC
LPC_FRAME#	O	CMOS	3.3V			LPC frame indicates the start of an LPC cycle	AL SOC
LPC_DRQ0#	I	CMOS	3.3V	3.3V		LPC serial DMA request not available	AL SOC
LPC_DRQ1#	I	CMOS	3.3V			LPC serial DMA request not available	AL SOC
LPC_SERIRQ	I/OD	CMOS	3.3V	3.3V	ePU = 10 KΩ	LPC serial interrupt	AL SOC
LPC_CLK	O	CMOS	3.3V		eSR = 10 Ω	LPC clock output - 33MHz nominal, functional strap option	AL SOC

2.13.8 LVDS / eDP

Signal Name LVDS	Pin Number	Signal Name eDP (Option)
LVDS_A0+	A71	eDP_TX2+
LVDS_A0-	A72	eDP_TX2-
LVDS_A1+	A73	eDP_TX1+
LVDS_A1-	A74	eDP_TX1-
LVDS_A2+	A75	eDP_TX0+
LVDS_A2-	A76	eDP_TX0-
LVDS_A_CK+	A81	eDP_TX3+
LVDS_A_CK-	A82	eDP_TX3-
LVDS_VDD_EN	A77	eDP_VDD_EN
LVDS_BKLT_EN	B79	eDP_BKLT_EN
LVDS_BKLT_CTRL	B83	eDP_BKLT_CTRL
LVDS_I2C_CK	A83	eDP_AUX+
LVDS_I2C_DAT	A84	eDP_AUX-
RSVD	A87	eDP_HPD

2.13.8.1 LVDS Flat Panel (mounting option, only available on modules with LVDS mounting option)

Signal	Pin Type	Signal Level	Power Rail	Remark / Tolerance	PU/PD/SR	Description	Source / Target
LVDS_A[0:3]+ LVDS_A[0:3]-	O	LVDS				LVDS Channel A differential pairs	ANX1122
LVDS_A_CK+ LVDS_A_CK-	O	LVDS				LVDS Channel A differential clock	ANX1122
LVDS_VDD_EN	O	CMOS	3.3V			LVDS panel power enable	ANX1122
LVDS_BKLT_EN	O	CMOS	3.3V			LVDS panel backlight enable	Embedded Controller
LVDS_BKLT_CTRL	O	CMOS	3.3V			LVDS panel backlight brightness control	Embedded Controller
LVDS_I2C_CK	O	CMOS	3.3V		ePU = 2.2 KΩ	I2C clock output for LVDS display use	ANX1122
LVDS_I2C_DAT	I/OD	CMOS	3.3V	3.3V	ePU = 2.2 KΩ	I2C data line for LVDS display use	ANX1122

2.13.8.2 eDP (mounting option, only available on modules with eDP mounting option)

Signal	Pin Type	Signal Level	Power Rail	Remark / Tolerance	PU/PD/SR	Description	Source / Target
eDP_TX[0:3]+ eDP_TX[0:3]-	O	PCIe		AC coupled off module		eDP differential pairs	AL SOC
eDP_VDD_EN	O	CMOS	3.3V	3.3V		eDP power enable	AL SOC
eDP_BKLT_EN	O	CMOS	3.3V	3.3V		eDP backlight enable	Embedded Controller
eDP_BKLT_CTRL	O	CMOS	3.3V	3.3V		eDP backlight brightness control	Embedded Controller
eDP_AUX+	I/O	PCIe		AC coupled off module		eDP_AUX+	AL SOC
eDP_AUX-	I/O	PCIe		AC coupled off module		eDP_AUX-	AL SOC
eDP_HPD	I	CMOS	3.3V	3.3V	ePD = 100 KΩ	Detection of Hot Plug / Unplug and notification of the link layer	AL SOC

2.13.9 Digital Display Interfaces

2.13.9.1 Overview Type10 DDI Video Type Mapping

	Signal	DP	HDMI/DVI (TMDS Signaling)
DDI0	DDI0_PAIR0+/-	DP0_LANE0+/-	TMDS0_DATA2+/-
	DDI0_PAIR1+/-	DP0_LANE1+/-	TMDS0_DATA1+/-
	DDI0_PAIR2+/-	DP0_LANE2+/-	TMDS0_DATA0+/-
	DDI0_PAIR3+/-	DP0_LANE3+/-	TMDS0_DATACLK+/-
	DDI0_HPD	DP0_HPD	HDMI0_HPD
	DDI0_CTRLCLK/DATA_AUX+/-	DP0_AUX+/-	HDMI0_CTRLCLK/DATA
	DDI0_DDC_AUX_SEL		

2.13.9.2 DisplayPort

Signal	Pin Type	Signal Level	Power Rail	Remark / Tolerance	PU/PD/SR	Description	Source / Target
DP0_LANE[0:3]+ DP0_LANE[0:3]-	O			AC coupled off module		DisplayPort Lane [0:3] differential pairs.	AL SOC
DP0_AUX+ DP0_AUX-	I/O			AC coupled on module	ePD = 100 KΩ ePU = 100 KΩ	DisplayPort Aux control channel differential pair	AL SOC
DP0_HPD	I	CMOS	3.3V	3.3V	ePD = 100 KΩ	DisplayPort Hot Plug Detect.	AL SOC
DDI0_DDC_AUX_SEL	I	CMOS	3.3V	3.3V	ePD = 1 MΩ	If this input is floating the AUX pair is used for the DP AUX+/- signals. If pulled high the AUX pair contains the CTRLCLK and CTRLDATA signals.	Carrier board logic circuit

2.13.9.3 HDMI / DVI

Signal	Pin Type	Signal Level	Power Rail	Remark / Tolerance	PU/PD/SR	Description	Source / Target
TMDS0_DATA[0:2]+ TMDS0_DATA[0:2]-	O	TMDS		AC coupled off module		HDMI/DVI TMDS Data [0:2] output differential pairs.	AL SOC
TMDS0_DATACLK+ TMDS0_DATACLK-	O	TMDS		AC coupled off module		HDMI/DVI TMDS Clock differential pairs.	AL SOC
HDMI0_CTRLCLK	I/O	CMOS	3.3V	3.3V	ePD = 100 KΩ	HDMI/DVI Control Clock. Shared with DP1_AUX+.	AL SOC
HDMI0_CTRLDATA	I/O	CMOS	3.3V	3.3V	ePU = 100 KΩ	HDMI/DVI Control Data. Shared with DP1_AUX-.	AL SOC
HDMI0_HPD	I	CMOS	3.3V	3.3V	ePD = 100 KΩ	HDMI/DVI Hot Plug Detect.	AL SOC
DDI0_DDC_AUX_SEL	I	CMOS	3.3V	3.3V	ePD = 1 MΩ	Pull to 3.3V on the Carrier with 100k Ohm resistor to configure the DDI1_AUX pair as the DDC channel.	Carrier board logic circuit

2.13.10 Serial Interface Signals

Signal	Pin Type	Signal Level	Power Rail	Remark / Tolerance	PU/PD/SR	Description	Source / Target
SER0_TX	O	CMOS	3.3V	12V, 7mA		General purpose serial port transmitter (output)	AL SOC
SER0_RX	I	CMOS	3.3V	12V	ePU = 47 KΩ	General purpose serial port receiver (input)	AL SOC
SER1_TX	O	CMOS	3.3V	12V, 7mA		General purpose serial port transmitter (output)	AL SOC
SER1_RX	I	CMOS	3.3V	12V	ePU = 47 KΩ	General purpose serial port receiver (input)	AL SOC

2.13.11 Miscellaneous

Signal	Pin Type	Signal Level	Power Rail	Remark / Tolerance	PU/PD/SR	Description	Source / Target
I2C_CK	I/O	CMOS	3.3V Sus	3.3V	ePU = 2.2 KΩ	General purpose I2C port clock output	AL SOC
I2C_DAT	I/O	CMOS	3.3V Sus	3.3V	ePU = 2.2 KΩ	General purpose I2C port data I/O line	AL SOC
SPKR	O	CMOS	3.3V	3.3V, 7mA		Output for audio enunciator - the "speaker" in PC-AT systems	AL SOC
BIOS_DIS[1]#	I	CMOS	3.3V		ePU = 10 KΩ	Module BIOS disable input	Carrier board logic circuit
BIOS_DIS[0]#	I	CMOS	3.3V		ePU = 10 KΩ	Module BIOS disable input, not connected	Carrier board logic circuit
WDT	O	CMOS	3.3V		ePD = 10 KΩ	Active high output indicating that a watchdog time-out has occurred.	Embedded Controller
FAN_PWMOUT	O	CMOS	3.3V			Fan speed control. Uses the Pulse Width Modulation (PWM) technique to control the fan’s RPM.	Embedded Controller
FAN_TACHIN	I	CMOS	3.3V		ePU = 10 KΩ	Fan tachometer input for a fan with a two pulse output.	Embedded Controller
TPM_PP	I	CMOS	3.3V	3.3V	ePD = 4.99 KΩ	Trusted Platform Module (TPM) Physical Presence pin. Active high.	TPM

ⓘ NOTICE: COM Express Specification R2.1 redefines the I2C bus to be in the suspend plane 3.3V_SUS rather than in the 3.3V plane.

2.13.12 Power and System Management

Signal	Pin Type	Signal Level	Power Rail	Remark / Tolerance	PU/PD/SR	Description	Source / Target
PWRBTN#	I	CMOS	3.3V Sus		ePU = 10 KΩ	Power button to bring system out of or into Suspend states.	Embedded Controller
SYS_RESET#	I	CMOS	3.3V Sus	3.3V	ePU = 10 KΩ	Reset button input.	Embedded Controller
CB_RESET#	O	CMOS	3.3V Sus	3.3V, 7mA		Reset output from module to Carrier Board. Active low. Issued by module chipset and may result from a low SYS_RESET# input, a low PWR_OK input, a VCC_12V power input that falls below the minimum specification, a watchdog timeout, or may be initiated by the module software.	AL SOC
PWR_OK	I	CMOS	3.3V Sus	12V	ePU = 47 KΩ	Power OK from main power supply. A high value indicates that the power is good.	Power logic circuit
SUS_STAT#	O	CMOS	3.3V Sus	3.3V		Indicates imminent suspend operation; used to notify LPC devices.	AL SOC
SUS_S3#	O	CMOS	3.3V Sus	3.3V, 24mA		Indicates system is in Suspend to RAM state. Active low output.	AL SOC
SUS_S4#	O	CMOS	3.3V Sus	3.3V, 24mA		Indicates system is in Suspend to Disk state. Active low output. Shorted to SUS_S5#.	AL SOC
SUS_S5#	O	CMOS	3.3V Sus	3.3V, 24mA		Indicates system is in Soft Off state. Also known as "PS_ON" and can be used to control an ATX power supply.	AL SOC
WAKE0#	I	CMOS	3.3V Sus	3.3V	ePU = 10 KΩ	PCI Express wake-up signal.	AL SOC
WAKE1#	I	CMOS	3.3V Sus	3.3V	ePU = 10 KΩ	General purpose wake up signal. May be used to implement wake-up on PS2 keyboard or mouse activity.	AL SOC
BATLOW#	I	CMOS	3.3V Sus	3.3V	ePU = 10 KΩ	Indicates that external battery is low.	AL SOC, Embedded Controller
LID#	I	CMOS	3.3V Sus	12V	ePU = 10 KΩ	LID switch. Low active signal used by ACPI operating system for LID switch.	AL SOC, Embedded Controller

Signal	Pin Type	Signal Level	Power Rail	Remark / Tolerance	PU/PD/SR	Description	Source / Target
SLEEP#	I	CMOS	3.3V Sus	12V	ePU = 10 KΩ	Sleep button. Low active signal used by ACPI operating system to bring the system to sleep state or wake it up again.	AL SOC, Embedded Controller
THRM#	I	CMOS	3.3V	3.3V	ePU = 10 KΩ	Input from off-module temperature sensor indicating an over-temp situation. Not supported.	AL SOC, Embedded Controller
THRMTRIP#	O	CMOS	3.3V	3.3V, 24mA	ePU = 10 KΩ	Active low output indicating that the CPU has entered thermal shutdown.	AL SOC, Embedded Controller
SMB_CK	I/O OD	CMOS	3.3V Sus	3.3V	ePU = 2.2 KΩ	System Management Bus bidirectional clock line. Power sourced through 3.3V standby rail.	AL SOC, Embedded Controller
SMB_DAT	I/O OD	CMOS	3.3V Sus	3.3V	ePU = 2.2 KΩ	System Management Bus bidirectional data line. Power sourced through 3.3V standby rail.	AL SOC, Embedded Controller
SMB_ALERT#	I	CMOS	3.3V Sus	3.3V	ePU =2.2 KΩ	System Management Bus Alert – active low input can be used to generate SMI# (System Management Interrupt) or to wake the system. Power sourced through 3.3V standby rail.	AL SOC, Embedded Controller

2.13.13 General Purpose I/O

Signal	Pin Type	Signal Level	Power Rail	Remark / Tolerance	PU/PD/SR	Description	Source / Target
GPI[0:3]	I	CMOS	3.3V	3.3V		General purpose input pins. Pulled high internally on the module. These signals are multiplexed with SDIO interface.	AL SOC
GPO[0:3]	O	CMOS	3.3V	3.3V		General purpose output pins. Upon a hardware reset, these outputs are low. These signals are multiplexed with SDIO interface.	AL SOC

2.13.14 SDIO

Signal	Pin Type	Signal Level	Power Rail	Remark / Tolerance	PU/PD/SR	Description	Source / Target
SDIO_CD# (GPO3)	I	CMOS	1.8V/3.3V	1.8V / 3.3V	iPU = 20 KΩ	SDIO Card Detect. This signal indicates when a SDIO/MMC card is present. This pin is mapped to GPO3 and used as an input when used for SD card support.	AL SOC
SDIO_CLK (GPO0)	O	CMOS	1.8V/3.3V	1.8V / 3.3V	iPU = 20 KΩ	SDIO Clock. With each cycle of this signal a one-bit transfer on the command and each data line occurs. This signal has maximum frequency of 48 MHz. This pin is mapped to GPO0.	AL SOC
SDIO_CMD (GPO1)	O	CMOS	1.8V/3.3V	1.8V / 3.3V	iPU = 20 KΩ	SDIO Command/Response. This signal is used for card initialization and for command transfers. During initialization mode this signal is open drain. During command transfer this signal is in push-pull mode. This pin is mapped to GPO1	AL SOC
SDIO_WP (GPO2)	I	CMOS	1.8V/3.3V	1.8V / 3.3V	iPU = 20 KΩ	SDIO Write Protect. This signal denotes the state of the write-protect tab on SD cards. This pin is mapped to GPO2 and used as an input when used for SD card support	AL SOC
SDIO_DAT[0:3] (GPI[0:3])	IO	CMOS	1.8V/3.3V	1.8V / 3.3V	iPU = 20 KΩ	SDIO Data lines. These signals operate in push-pull mode. These pins are mapped to GPI[0:3].	AL SOC

ⓘ NOTICE: Bus Speed Mode SDIO 3.0 (UHS-I) supported.

2.13.15 SPI Interface

Signal	Pin Type	Signal Level	Power Rail	Rem. / Tol.	PU/PD/SR	Description	Source / Target
SPI_CS#	O	CMOS	**1.8V Sus**	**1.8V**	ePU = 47 KΩ eSR = 22 Ω	Chip select for Carrier Board SPI - may be sourced from chipset SPI0 or SPI1.	AL SOC
SPI_MISO	I	CMOS	**1.8V Sus**	**1.8V**	eSR = 22 Ω	Data in to Module from Carrier SPI.	AL SOC
SPI_MOSI	O	CMOS	**1.8V Sus**	**1.8V**	eSR = 22 Ω	Data out from Module to Carrier SPI.	AL SOC
SPI_CLK	O	CMOS	**1.8V Sus**	**1.8V**	eSR = 22 Ω	Clock from Module to Carrier SPI.	AL SOC
SPI_POWER	O	Power	**1.8V Sus**			Power supply for Carrier Board SPI – sourced from Module – nominally 3.3V. The Module shall provide a minimum of 100mA on SPI_POWER. Carriers shall use less than 100mA of SPI_POWER. SPI_POWER shall only be used to power SPI devices on the Carrier.	
BIOS_DIS [1:0]#	I	CMOS	3.3V Sus	3.3V	ePU = 10 KΩ	Selection straps to determine the BIOS boot device.	

BIOS_DIS[1:0]#		SPI_CS1# Destination	SPI_CS0# Destination	Carrier SPI_CS#	SPI Descriptor	BIOS Entry
1	1	Module	Module	HIGH	Module	SPI0/SPI1
1	0	Module	Module	HIGH	Module	Carrier FWH
0	1	Module	Carrier	SPI0	Carrier	SPI0/SPI1
0	0	Carrier	Module	SPI1	Module	SPI0/SPI1

ⓘ NOTICE: SPI power rail is 1.8V.

2.13.16 Module Type Definition

Signal	Pin Type	Signal Level	Power Rail	Remark / Tolerance	PU/PD/SR	Description	Source / Target
TYPE10#	O			47K pull down COM.0 Rev 2.1 Module Type 10		Dual use pin. Indicates to the Carrier Board that a Type 10 Module is installed. Indicates to the Carrier that a Rev 1.0/2.0 Module is installed TYPE10# NC Pin-out R2.0 PD Pin-out Type 10 pull down to ground with 4.7K resistor 12V Pin-out R1.0 This pin is reclaimed from the VCC_12V pool. In R1.0 Modules this pin will connect to other VCC_12V pins. In R2.0 this pin is defined as a no connect for types 1-6. A Carrier can detect a R1.0 Module by the presence of 12V on this pin. R2.0 Module types 1-6 will no connect this pin. Type 10 Modules shall pull this pin to ground through a 47K resistor.	Carrier board logic

2.13.17 Power and GND

Signal	Pin Type		Signal Level	Power Rail	Remark / Tolerance	PU/PD/SR	Description	Source / Target
VCC_12V	Power			12V (±5%)			Primary power input: +12V (±5%) Wide input range 4.75 – 20.0V	Voltage Regulators
VCC_5V_SBY	Power			5V (±5%)			Standby power input: +5.0V (±5%) If VCC5_SBY is used, all available VCC_5V_SBY pins on the connector(s) shall be used. Only used for standby and suspend functions. May be left unconnected if these functions are not used in the system design.	VCC3.3V SUS regulator
VCC_RTC	Power						Real-time clock circuit-power input : +3.0V (+2.5V to +3.3V)	AL SOC
GND	Power						Ground - DC power and signal and AC signal return path. All available GND connector pins shall be used and tied to Carrier Board GND plane.	

2.14 Pin List

MSC C10M-AL Module (Type 10) Pin List:

Row A		Row B	
A1	GND (FIXED)	B1	GND (FIXED)
A2	GBE0_MDI3-	B2	GBE0_ACT#
A3	GBE0_MDI3+	B3	LPC_FRAME#
A4	GBE0_LINK100#	B4	LPC_AD0
A5	GBE0_LINK1000#	B5	LPC_AD1
A6	GBE0_MDI2-	B6	LPC_AD2
A7	GBE0_MDI2+	B7	LPC_AD3
A8	GBE0_LINK#	B8	LPC_DRQ0#
A9	GBE0_MDI1-	B9	LPC_DRQ1#
A10	GBE0_MDI1+	B10	LPC_CLK
A11	GND (FIXED)	B11	GND (FIXED)
A12	GBE0_MDI0-	B12	PWRBTN#
A13	GBE0_MDI0+	B13	SMB_CK
A14	GBE0_CTREF	B14	SMB_DAT
A15	SUS_S3#	B15	SMB_ALERT#
A16	SATA0_TX+	B16	SATA1_TX+
A17	SATA0_TX-	B17	SATA1_TX-
A18	SUS_S4#	B18	SUS_STAT#
A19	SATA0_RX+	B19	SATA1_RX+
A20	SATA0_RX-	B20	SATA1_RX-
A21	GND (FIXED)	B21	GND (FIXED)
A22	USB_SSRX0-	B22	USB_SSTX0-

Row A		Row B	
A23	USB_SSRX0+	B23	USB_SSTX0+
A24	SUS_S5#	B24	PWR_OK
A25	USB_SSRX1-	B25	USB_SSTX1-
A26	USB_SSRX1+	B26	USB_SSTX1+
A27	BATLOW#	B27	WDT
A28	(S)ATA_ACT#	B28	AC/HDA_SDIN2
A29	AC/HDA_SYNC	B29	AC/HDA_SDIN1
A30	AC/HDA_RST#	B30	AC/HDA_SDIN0
A31	GND (FIXED)	B31	GND (FIXED)
A32	AC/HDA_BITCLK	B32	SPKR
A33	AC/HDA_SDOUT	B33	I2C_CK
A34	BIOS_DIS0# n. c.	B34	I2C_DAT
A35	THRMTRIP#	B35	THRM#
A36	USB6-	B36	USB7-
A37	USB6+	B37	USB7+
A38	USB_6_7_OC#	B38	USB_4_5_OC#
A39	USB4-	B39	USB5-
A40	USB4+	B40	USB5+
A41	GND (FIXED)	B41	GND (FIXED)
A42	USB2-	B42	USB3-
A43	USB2+	B43	USB3+
A44	USB_2_3_OC#	B44	USB_0_1_OC#
A45	USB0-	B45	USB1-
A46	USB0+	B46	USB1+

Row A		Row B	
A47	VCC_RTC	B47	EXCD1_PERST#
A48	EXCD0_PERST#	B48	EXCD1_CPPE#
A49	EXCD0_CPPE#	B49	SYS_RESET#
A50	LPC_SERIRQ	B50	CB_RESET#
A51	GND (FIXED)	B51	GND (FIXED)
A52	RSVD	B52	RSVD
A53	RSVD	B53	RSVD
A54	GPI0	B54	GPO1
A55	RSVD	B55	RSVD
A56	RSVD	B56	RSVD
A57	GND	B57	GPO2
A58	PCIE_TX3+	B58	PCIE_RX3+
A59	PCIE_TX3-	B59	PCIE_RX3-
A60	GND (FIXED)	B60	GND (FIXED)
A61	PCIE_TX2+	B61	PCIE_RX2+
A62	PCIE_TX2-	B62	PCIE_RX2-
A63	GPI1	B63	GPO3
A64	PCIE_TX1+	B64	PCIE_RX1+
A65	PCIE_TX1-	B65	PCIE_RX1-
A66	GND	B66	WAKE0#
A67	GPI2	B67	WAKE1#
A68	PCIE_TX0+	B68	PCIE_RX0+
A69	PCIE_TX0-	B69	PCIE_RX0-
A70	GND (FIXED)	B70	GND (FIXED)

Row A		Row B	
A71	LVDS_A0+	B71	DDI0_PAIR0+
A72	LVDS_A0-	B72	DDI0_PAIR0-
A73	LVDS_A1+	B73	DDI0_PAIR1+
A74	LVDS_A1-	B74	DDI0_PAIR1-
A75	LVDS_A2+	B75	DDI0_PAIR2+
A76	LVDS_A2-	B76	DDI0_PAIR2-
A77	LVDS_VDD_EN	B77	DDI0_PAIR4+ n. c.
A78	LVDS_A3+	B78	DDI0_PAIR4- n. c.
A79	LVDS_A3-	B79	LVDS_BKLT_EN
A80	GND (FIXED)	B80	GND (FIXED)
A81	LVDS_A_CK+	B81	DDI0_PAIR3+
A82	LVDS_A_CK-	B82	DDI0_PAIR3-
A83	LVDS_I2C_CK	B83	LVDS_BKLT_CTRL
A84	LVDS_I2C_DAT	B84	VCC_5V_SBY
A85	GPI3	B85	VCC_5V_SBY
A86	RSVD	B86	VCC_5V_SBY
A87	eDP_HPD	B87	VCC_5V_SBY
A88	PCIE0_CK_REF+	B88	BIOS_DIS1#
A89	PCIE0_CK_REF-	B89	DD0_HPD
A90	GND (FIXED)	B90	GND (FIXED)
A91	SPI_POWER	B91	DDI0_PAIR5+ n. c.
A92	SPI_MISO	B92	DDI0_PAIR5- n. c.
A93	GPO0	B93	DDI0_PAIR6+ n. c.
A94	SPI_CLK	B94	DDI0_PAIR6- n. c.

Row A		Row B	
A95	SPI_MOSI	B95	DDI0_DDC_AUX_SEL
A96	TPM_PP	B96	USB_HOST_PRSNT
A97	TYPE10#	B97	SPI_CS#
A98	SER0_TX	B98	DDI0_CTRLCLK_AUX+
A99	SER0_RX	B99	DDI0_CTRLDATA_AUX-
A100	GND (FIXED)	B100	GND (FIXED)
A101	SER1_TX	B101	FAN_PWNOUT
A102	SER1_RX	B102	FAN_TACHIN
A103	LID#	B103	SLEEP#
A104	VCC_12V	B104	VCC_12V
A105	VCC_12V	B105	VCC_12V
A106	VCC_12V	B106	VCC_12V
A107	VCC_12V	B107	VCC_12V
A108	VCC_12V	B108	VCC_12V
A109	VCC_12V	B109	VCC_12V
A110	GND (FIXED)	B110	GND (FIXED)

▨	= not supported on MSC C10M-AL modules.

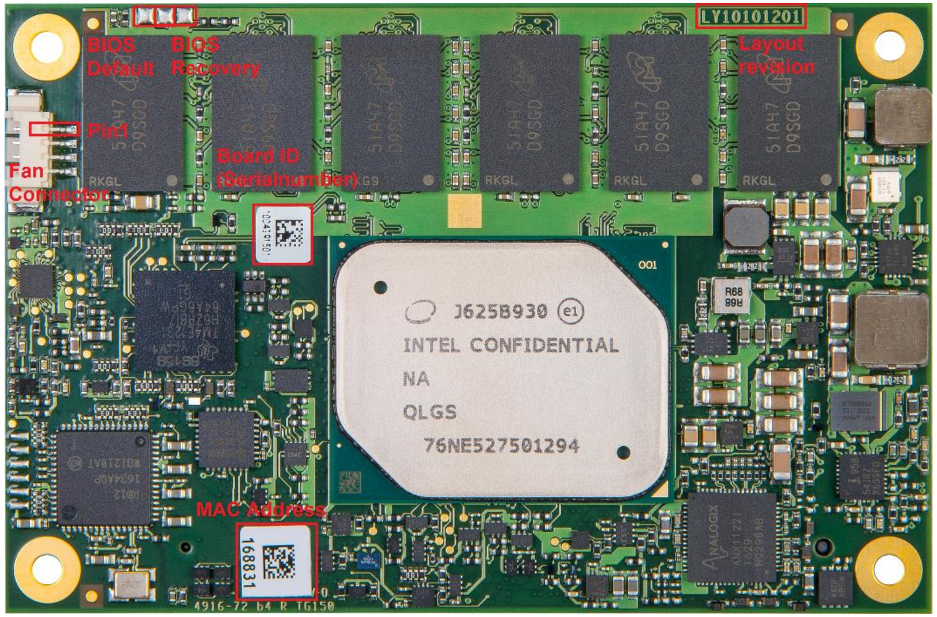
3 Jumpers and Connectors

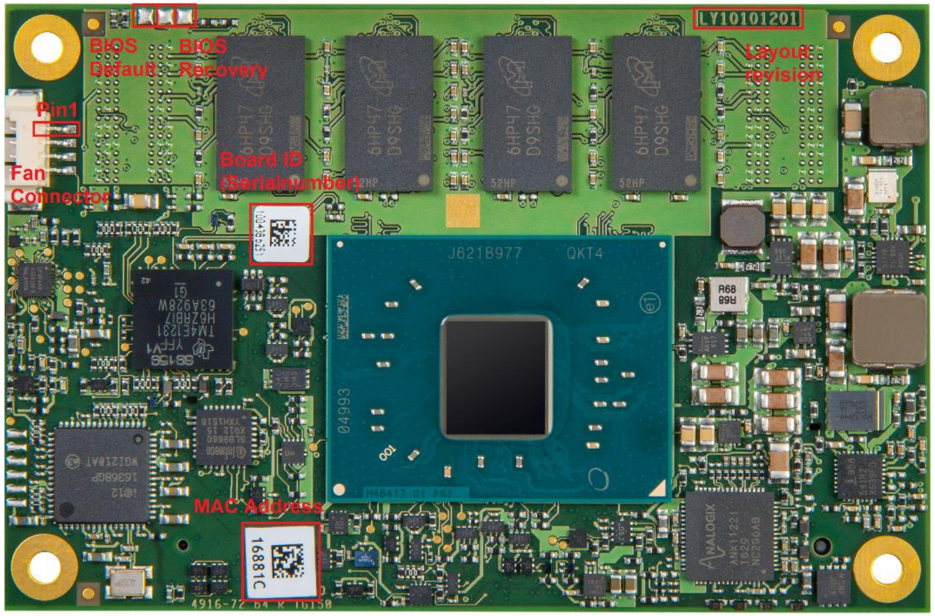
3.1 Jumpers

There are two jumpers available on the module:

- BIOS Default: By shorting the pins of this jumper during boot, the values of the BIOS setup will be reset to default values.
- BIOS Recovery: By shorting the pins of this jumper during boot the system is forced into crisis recovery mode. For more information see chapter 6.18.

These jumpers are located at the top side of the board on the edge of the PCB (see photo).





3.2 Fan Connector

The connector of the fan is a mounting option and is located at top side of the CPU module, directly beneath the CPU:

The following connector type is used:

- Molex 53261-0471

The fan itself should be equipped with a Molex 51021-400 connector and one of the following contact types:

- Molex 50058 Crimp Terminal (28-32 AWG),
- Molex 50079 Crimp Terminal (26-28 AWG)

The pinning is as following (numbering from right to left):

Pin	Signal	Description
1	GND	GND
2	V12FAN	+12V fan supply voltage.
3	TACHO	Input for the tacho signal from the fan (open collector); two pulses / rotation
4	PWM	PWM output signal for fan speed control.

⚠ **Caution:** Using the power supply wide input range at more than +12V can damage the fan. The correct function of the fan is not guaranteed below +12V.

4 Watchdog

The C10M-AL board has a watchdog function implemented by an embedded controller.

The watchdog can be enabled and configured in the BIOS Setup.

If the watchdog is enabled a counter is started which generates a reset if it is not retriggered within a programmable time window.

The time delay starts as soon as it is enabled in the BIOS.

MSC provides a software API which gives the application software access to the Watchdog functionality if needed.

5 System Resources

		Interrupts of Controller								
Slot Number	Dev /	Bus #	PIRQ 0	PIRQ 1	PIRQ 2	PIRQ 3	PIRQ 4	PIRQ 5	PIRQ 6	PIRQ 7
(or Onboard Device)	Function		(INT A)	(INT B)	(INT C)	(INT D)	(INT E)	(INT F)	(INT G)	(INT H)
IGD	0x02/0	0				x				
IUNIT	0x03/0	0						x		
PMC	0x0D/1	0	x							
HDA	0x0E/0	0	x							
CSE	0x0F/0	0					x			
ISH	0x11/0	0					x			
SATA	0x12/0	0	x							
xHCI	0x15/0	0		x						
XDCI	0x15/1	0			x					
I2C4	0x17/0	0		x						
I2C6	0x17/2	0			x					
UART0	0x18/0	0	x							
UART1	0x18/1	0		x						
SPI0	0x19/0	0	x							
SDCard	0x1B/0	0		x						
EMMC	0x1C/0	0			x					
SMBus Controller	0x1f/1	0				x				
PCIE Root Port 0	0x13/0	0					a	b	c	d
PCIE Root Port 1	0x13/1	0					d	a	b	c
PCIE Root Port 2	0x13/2	0					c	d	a	b
PCIE Root Port 3	0x13/3	0					b	c	d	a
PCIE Root Port 4 (connected to GBE Lan)	0x14/0	0							x	

5.1 SMB Address Map

Device	Address *)
SO-DIMM 0 SPD EEPROM	A0h / 50h
CMOS Backup EEPROM	A8h / 54h AAh / 55h
Embedded Controller	C0h / 60h
ANX1122	50h/ 28h
ANX1122	8Ch/ 46h

*) 8 bit address (with R/W) / 7 bit address (without R/W)

6 BIOS

6.1 Introduction

This guide describes the AMI Aptio Setup Startup screen and contains information on how to access Aptio setup to modify the settings which control AMI pre-OS (operating system) functions.

6.2 Startup Screen Overview

The AMI Aptio Startup screen is a graphical user interface (GUI) that is included in AMI Aptio products. The default bios behavior is to show an informational text screen during bios POST phase, but the graphical boot screen can be enabled in the bios setup. The standard boot screen is a black screen without any logo.

6.3 Activity Detection Background

While the startup screen is displayed, press the Setup Entry key [ESC] or [DEL]. The system acknowledges the input, and at the end of POST, the screen clears and setup launches.

Note:
By pressing [F10] during POST system will display a Boot Menu for directly booting a selected device.

6.4 Aptio Setup Utility

With the AMI Aptio Setup program, you can modify Aptio settings and control the special features of your computer. The setup program uses a number of menus for making changes and turning the special features on or off. This chapter provides an overview of the setup utility and describes at a high-level how to use it.

6.5 Configuring the System BIOS

To start the AMI Aptio Setup utility, press [ESC] or [DEL] to launch Setup. The setup main menu appears.

6.6 BIOS Menu Structure

The BIOS Menu is structured in the following way:

Main	Advanced	Chipset	Security	Boot	Save & Exit
Board Info	Trusted Computing	Flat Panel Configuration	Setup Administrator Password	Boot Configuration Advanced Boot Device Selection Boot Option Priorities	Save Options Default Options Boot Override
Hardware Monitoring	ACPI Settings	North Bridge	User Password		
System Information	SMART Settings	South Bridge	HDD Security Configuration		
Firmware Update	Serial Port Console Redirection	Uncore Configuration	Secure Boot		
	CPU Configuration	South Cluster Configuration			
	AMI Graphic Output Protocol Policy				
	PCI Subsystem Configuration				
	Network Stack Configuration				
	CSM Configuration				
	NVMe Configuration				
	SDIO Configuration				
	USB Configuration				
	Security Configuration				
	SIO WB627 Configuration				
	EC Hardware Monitoring				
	EC Features Configuration				
	Module-specific Initialization				

Main	Advanced	Chipset	Security	Boot	Save & Exit
	System Component				

6.6.1 Menu Bar

The Menu Bar at the top of the window lists these selections:

Menu Items	Description
Main	Use this menu for basic system information.
Advanced	Use this menu to set the Advanced Features available on your system’s chipset.
Chipset	Use this menu to set Chipset Features.
Security	Use this menu to set User and Supervisor Passwords and the Backup and Virus-Check reminders.
Boot	Use this menu to set the boot order in which the BIOS attempts to boot to OS.
Save & Exit	Saves and Exits the Aptio setup utility.

Use the left and right arrow keys on your keyboard to make a menu selection.

6.6.2 Legend Bar

Use the keys listed in the legend bar on the right side of the screen to make your selections, or to exit the current menu. The following table describes the legend keys and their alternates:

Key	Function
Left and right arrow keys	Select Screen
Up and down arrow keys	Select Item
Enter	Select
+/-	Change Option
F1	General Help window
F2	Previous Values
F3	Optimized Defaults
F4	Save and Exit
Esc	Exit submenu / Exit Setup utility without saving

Select an item

To select an item, use the arrow keys to move the cursor to the field you want. Then use the plus-and-minus value keys to select a value for that field. Alternatively the Enter key can be used to select a value from a Pop Up menu. The Save Values commands in the Exit Menu save the values currently displayed in all the menus.

Display a submenu

To display a submenu, use the arrow keys to move the cursor to the sub menu you want. Then press Enter. A pointer marks all submenus.

6.7 Main Menu

You can make the following selections on the Main Menu itself. Use the sub menus for other selections.

Feature	Options	Description
BIOS Information	Informative	Shows Information
BIOS Vendor	Informative	Shows the Bios Vendor
Core Version	Informative	Shows the Aptio Core Version
Compliancy	Informative	Shows the UEFI Compliance Version
Project Version	Informative	Shows the Project Version
Build Date and Time	Informative	Shows the Build Date
Access Level	Informative	This feature shows what kind of user has entered the Aptio setup. It depends on the Security Tab if an Administrator and/or User password is set.
Board Info	Submenu	Shows board specific information
Hardware Monitoring	Submenu	Shows the hardware sensors monitoring
System Information	Submenu	Shows System Information
Firmware Update	Submenu	MSC Firmware Update Submenu
System Date	Enter Date (MM:DD:YYYY)	Set the system date on the real time clock.
System Time	Enter Time (HH:MM:SS)	Set the system time on the real time clock.

6.7.1 Board Info

Feature	Options	Description
Manufacturer	Informative	Avnet Embedded GmbH (or earlier: MSC Technologies GmbH)
Board Name	Informative	Shows the board name
Board Revision	Informative	Shows the board revision
BIOS Version	Informative	Shows the bios version
Serial Number	Informative	Shows the boards serial number
Boot Counter	Informative	Shows the amount of boots
Operating Time (hh:mm)	Informative	Shows the whole operating time (in S0) of the module
CPU Min Temperature	Informative	Shows the lowest temperature of the CPU ever measured
CPU Max Temperature	Informative	Shows the highest temperature of the CPU ever measured
Board Min Temperature	Informative	Shows the lowest temperature of the board ever measured
Board Max Temperature	Informative	Shows the highest temperature of the board ever measured
Memory Min Temperature	Informative	Shows the lowest temperature of memory ever measured
Memory Max Temperature	Informative	Shows the highest temperature of memory ever measured
EC Bootloader Version	Informative	Shows the bootloader version of the EC
EC Firmware Version	Informative	Shows the firmware version of the EC
EC BX Version	Informative	Shows the version of the battery extension of EC
EC CX Version	Informative	Shows the version of the customer extension of EC
Onboard Lan MAC Adress	Informative	Shows the onboard Lan MAC Adress
UUID	Informative	Shows the UUID

6.7.2 Hardware Monitoring

Feature	Options	Description
CPU Temperature	Informative	Shows CPU temperature Also supported in EAPI **Note:** CPU temperature is measured close to the CPU and does not reflect CPU die temperature
Memory Temperature	Informative	Shows CPU temperature
Board Temperature	Informative	Shows the board temperature
VCore	Informative	Shows the VCore voltage
3.3V	Informative	Shows the 3.3V voltage
5V	Informative	Shows the 5V voltage
5V Standby	Informative	Shows the 5V Standby voltage
12V	Informative	Shows the 12V voltage
Vbat	Informative	Shows the voltage of the RTC
CPU Fan Speed	Informative	Shows the current CPU fan speed
System Fan Speed	Informative	Shows the current System fan speed

6.7.3 System Information

Feature	Options	Description
BXT SOC MRC Version PUNIT FW PMC FW TXE FW ISH FW GOP CPU Flavor Memory Information Total Memory Memory Speed Error Correction	Informative	Shows several information e.g TXE Version, GOP Driver Version,…

6.7.4 Firmware Update

Feature	Options	Description
Configure Update	Bios Only, Entire Flash	BIOS only: Update BIOS Region, Entire Flash: Update Entire Flash
Preserve SMBIOS Variable	Enabled, Disabled	If Enabled, restore SMBIOS Variables (DMI Table)
Preserve Boot Option Priorities	Enabled, Disabled	If enabled, restore Boot Option Priorities after Firmware update. This option does not restore the Advanced Boot Device Selection in Boot Menu
Verbose Mode	Enabled, Disabled	If Enabled, Firmware Update displays some messages on the console

Feature	Options	Description
Beep Mode	Enabled, Disabled	If Enabled, Firmware Update is reported by Beep Codes
Network Configuration	Submenu	Configure the network device for loading the flash image from network
Preserve Network Paramater	Enabled, Disabled	If Enabled, preserve Network Settings
Start Firmware Update		Press Enter to Start a Firmware Update. The BIOS Image has to be placed into the correct directory. See above. ⚠ **Caution: Make sure if POST Watchdog is enabled, a higher timeout as 60s is selected or disable POST Watchdog for the Bios Update, otherwise Bios Update can become corrupt and system won't boot again.** **On first boot or after Bios Update the system takes a little bit longer to boot as normal (e.g Memory detection)**
Trusted Update	Informative : Inactive / Active	Indicates trusted bios update is active or not. If active, the update is only possible with a signed image file. See chapter 6.19 for more information

See chapter 6.13 for more information about how to update system bios.

6.7.5 Network Configuration

Feature	Options	Description
Network Device	0: Lan 0 ; …	Select the network device for firmware update
Local Adress Mode	Static, DHCP	Select local address mode Static: enter station address, subnetmask and gateway DHCP: get information from DHCP

Feature	Options	Description
Local IP Adress	Local IP Adress	Enter local IP address in dotted-decimal notation Note: only visible if local address mode is set to static
Local NetMask	Local NetMask	Enter subnet mask in dotted-decimal notation Note: only visible if local address mode is set to static
Default Gateway Address	Dafault Gateway Adress	Enter default gateway address in dotted-decimal notation Note: only visible if local address mode is set to static
Optional DNS Server 1	DNS Server 1	Enter optional DNS Server- Entry 0 in dotted-decimal notation Note: only visible if local address mode is set to static
Optional DNS Server 2	DNS Server 2	Enter optional DNS Server- Entry 0 in dotted-decimal notation Note: only visible if local address mode is set to static
Optional DNS Server 3	DNS Server 3	Enter optional DNS Server- Entry 0 in dotted-decimal notation Note: only visible if local address mode is set to static
Optional DNS Server 4	DNS Server 4	Enter optional DNS Server- Entry 0 in dotted-decimal notation Note: only visible if local address mode is set to static
Update Network Protocol	TFTP, HTTP	Enter the Update Network Protocol
Server Adress Mode	Manual. DHCP	Select Server Address Mode. Static: enter server address DHCP: get the server address via DHCP
TFTP Server	Server Name	Enter TFTP server name or address in dotted-decimal notation
Image File Name Mode	Manual	Flash Image File Name Mode Manual : enter file name manually via DHCP Auto: generate a platform specific name
Image File Path/Name	Image File Path/Name	Enter flash image file path. Format path/filename

See chapter 6.13 for more information about how to update system bios.

6.8 Advanced Menu

Feature	Options	Description
Trusted Computing	Submenu	Trusted Computing (TPM)
ACPI Settings	Submenu	System ACPI Parameters
Smart Settings	Submenu	Smart Settings
Serial Port Console Redirection	Submenu	Serial Port Console Redirection
CPU Configuration	Submenu	CPU Configuration Parameters
AMI Graphic Output Protocol Policy	Submenu	User Select Monitor Output by Graphic Output
PCI Subsystem Settings	Submenu	PCI Subsystem Settings
Network Stack Configuration	Submenu	Configuration for UEFI Network boot
CSM Configuration	Submenu	CSM configuration: Enable/Disable, Option ROM execution settings, etc.
NVMe	Submenu	NVMe Device Option Settings
SDIO Configuration	Submenu	SDIO Configuration settings
USB Configuration	Submenu	USB Configuration settings
Security Configuration	Submenu	Security Configuration settings (TXE)
EC Hardware Monitoring	Submenu	Fan Configuration settings
EC Feature Configuration	Submenu	EC Feature Configuration
Module-specific Initialization	Submenu	Module-specific Initialization
System Component	Submenu	System Component

6.8.1 Trusted Computing (TPM)

Feature	Options	Description
Security Device Support	Enable, Disable	Enables or Disables BIOS support for security device. O.S. will not show Security Device. TCG EFI protocol and INT1A interface will not be available
SHA-1 PCR Bank	Enable, Disable	Enable or disable SHA-1 PCR Bank
SHA256 PCR Bank	Enable, Disable	Enable or disable SHA256 PCR Bank
Pending operation	None, TPM Clear	Schedule an Operation for the Security Device. NOTE: Your Computer will reboot during restart in order to change State of Security Device
Platform Hierarchy	Enable, Disable	Enable or Disable Platform Hierarchy
Storage Hierarchy	Enable, Disable	Storage Hierarchy
Endorsement Hierarchy	Enable, Disable	Enable or Disable Endorsement Hierarchy
TPM2.0 UEFI Spec Version	TCG_1.2 ; TCG_2	Select the TCG2 Spec Version Support, TCG_1_2: the Compatible mode for Win8/Win10, TCG_2: Support new TCG2 protocol and event format for Win10 or later
Physical Presence Spec Version	1.2 ; 1.3	Select to Tell O.S. to support PPI Spec Version 1.2 or 1.3. Note some HCK tests might not support 1.3.

6.8.2 ACPI Settings

Feature	Options	Description
Native PCIE Enable	Enabled Disabled	PCI Express Native Support Enable/Disable.
Hibernation Support	Enabled Disabled	Enables or disables system ability to Hibernate (OS/S4 Sleep State). This option may not effective with some OS.

Feature	Options	Description
ACPI Sleep State	Suspend Disabled S3 (Suspend to RAM)	Enables or Disabled System ability to enter S3 state (Suspend). This option may be not effective with some OS.
Lock Legacy Resources	Enabled Disabled	Set to enabled to prevent the OS from reconfiguring the resources of the SIO device through ACPI.

6.8.3 SMART Settings

Feature	Options	Description
SMART Self Test	Enabled, Disabled	Run SMART Self Test on all HDDs during POST

6.8.4 Serial Port Console Redirection

Feature	Options	Description
Com 0 and 1 Console Redirection	Enabled Disabled	Console Redirection Enable or Disable
Console Redirection settings Com 0 and 1	Submenu	The settings specify how the host computer and the remote computer (which the user is using) will exchange data. Both computers should have the same or compatible settings.
Com 4 and 5 Console Redirection	Enabled Disabled	Console Redirection Enable or Disable
Com 4 and 5 Console Redirection	Submenu	The settings specify how the host computer and the remote computer (which the user is using) will exchange data. Both computers should have the same or compatible settings.
Legacy Console Redirection	Submenu	Legacy Console Redirection Settings
Serial Port for Out-of Band	Enabled	Console Redirection Enable or Disable

Feature	Options	Description
Management/Windows Emergency Management Service (EMS) Console Redirection	Disabled	
Console Redirection Settings	Submenu	The settings specify how the host computer and the remote computer (which the user is using) will exchange data. Both computers should have the same or compatible settings.

6.8.5 Console Redirection Submenu

Feature	Options	Description
Terminal Type	ANSI, VT100, VT100+, VT-UTF8	Emulation: ANSI: Extended ASCII char set. VT100: ASCII char set. VT100+: Extends VT100 to support color, function keys, etc. VT-UTF8: Uses UTF8 encoding to map Unicode chars onto 1 or more bytes.
Bits per second	9600, 19200, 38400, 57600, 115200	Selects serial port transmission speed. The speed must be matched on the other side. Long or noisy lines may require lower speeds.
Data Bits	7, 8	Data Bits
Parity	None, Even, Odd, Mark, Space	A parity bit can be sent with the data bits to detect some transmission errors. Even: parity bit is 0 if the number of 1's in the data bits is even. Odd: parity bit is 0 if number of 1's in the data bits is odd. Mark: parity bit is always 1. Space: Parity bit is always 0. Mark and Space Parity do not allow for error detection. They can be used as an additional data bit.
Stop Bits	1,2	Stop bits indicate the end of a serial data packet. (A start bit indicates the beginning). The standard setting is 1 stop bit. Communication with slow devices may require more than 1 stop bit.
Flow Control	None, Hardware RTS/CTS,	Flow control can prevent data loss from buffer overflow. When sending data, if the receiving buffers are full, a 'stop' signal can be sent to stop the data flow. Once the buffers are empty, a 'start' signal can be sent to re-start the flow. Hardware flow control uses two wires to send start/stop signals.

Feature	Options	Description
VTUF8 Combo Key Support	Enabled, Disabled,	Enable VT-UF8 Combination Key Support for ANSI/VT100 terminals
Recorder Mode	Disabled, Enabled	With this mode enabled only text will be sent. This is to capture Terminal data.
Resolution 100x31	Disabled, Enabled	Enables or disables extended terminal resolution
Legacy OS Redirection	80x24, 80x25	On Legacy OS, the number of rows and Columns supported redirection
Putty KeyPad	VT100, Linux, XTERMR6, SCO, ESCN, VT400	Select FunctionKey and KeyPad on Putty.

6.8.6 CPU Configuration

Note: Dependent on used CPU, available setup options may vary!!!

Feature	Options	Description
Socket 0 CPU Information	Informative	See CPU relevant Informations in this submenu
CPU Power Management	Submenu	CPU Power Management options
Active Processor Cores	Enabled, Disabled	Number of cores to enable in each processor package.
Core 0	Enabled, Disabled	Core 0 Enable
Core 1	Enabled, Disabled	Core 1 Enable/Disable
Core 2	Enabled, Disabled	Core 2 Enable/Disable
Core 3	Enabled, Disabled	Core 3 Enable/Disable

Feature	Options	Description
Intel Virtualization Technology	Enabled, Disabled	When enabled, a VMM can utilize the additional hardware capabilities provided by Vanderpool Technology
VT-d	Enabled, Disabled	Enable/Disable CPU VT-d
Monitor Mwait	Enabled, Disabled	Enable/Disable Monitor Mwait.

6.8.7 CPU Power Management Submenu

Feature	Options	Description
EIST	Enabled Disabled	Enable/Disable Intel SpeedStep ⓘ NOTE **:** If disabled, System runs with nominal clock only. On resume from S3 the clock will be fixed to 800 MHz. Recommendation is not to use S3 if EIST is disabled**.**
Turbo Mode	Enabled Disabled	Enable/Disable Turbo Mode
Boot performance mode	Max Performance, MaxBattery	Select the performance state that the BIOS will set before OS handoff
C-States	Enabled Disabled	Enable/Disable C States
Enhanced C-states	Enabled Disabled	Enable/Disable C1E. When enabled, CPU will switch to minimum speed when all cores enter C-State.
Max Package C State	C0, PC1, PC2	Controls the Max Package C State that the processor will support.
Max Core C State	C1, C6, C7, C8, C9, C10, unlimited, Fused Value	This option controls the Max Core C State that cores will support.
C-State Auto Demotion	C1, Disabled	Configure C-State Auto Demotion
C-State Un-demotion	C1, Disabled	Configure C-State Un-demotion
Power Limit 1 Enable	Enabled Disabled	Enable/Disable Power Limit 1
Power Limit 1 Clamp Mode	Enabled Disabled	Enable/Disable Power Limit 1 Clamp Mode
Power Limit 1 Power	Auto, 6-25	Power Limit 1 in Watts. Auto will program Power Limit 1 based on silicon default support value
Power Limit 1 Time Window	Auto, 1-128	Power Limit 1 Time Window Value in Seconds. Auto will program Power Limit 1 Time Window based on silicon default support value

6.8.8 AMI Graphic Output Protocol Policy

Feature	Options	Description
Output Select	EDP1 (LVDS), DP1, DP2	Select Output Interface

ⓘ **NOTICE**: Be sure you have a LVDS connected if you switch to LVDS output because the output change is instantly. If you need to do a blind reset of the output you have to press Enter again, then Up or Down, then Enter.

If you need to do a blind reset from after entering setup, press 1x Right, then 5x Down, 2x Enter, 1x Down, 1x Enter.

6.8.9 PCI Subsystem

Feature	Options	Description
Above 4G Decoding	Enabled Disabled	Globally Enables or Disables 64-bit capable Devices to be Decoded in Above 4G Adress Space (Only if System Supports 64-bit PCI Decoding).
SR-IOV Support	Enabled Disabled	If system has SR-IOV capable PCIe Devices, this option Enables or Disables Single Root IO Virtualization Support
BME-DMA Mitigation	Enabled Disabled	Re-enable Bus Master Attribute disabled during PCI enumeration for PCI Bridges after SMM Locked
Hot-Plug Support	Enabled Disabled	Globally Enables or Disables Hot-Plug support for the entire System. If system has Hot-Plug capable Slots and this option set to Enabled, it provides a Setup screen for selecting PCI resurce padding for Hot-Plug.

6.8.10 Network Stack Configuration

Feature	Options	Description
Network Stack	Enabled, Disabled	Enable/Disable UEFI Network Stack
IPv4 PXE Support	Enabled, Disabled	Enable Ipv4 PXE Boot Support. If disabled IPV4 PXE boot option will not be created
Ipv4 HTTP Support	Enabled, Disabled	Enable Ipv4 HTTP Boot Support. If disabled IPV4 HTTP boot option will not be created
IPv6 PXE Support	Enabled, Disabled	Enable Ipv6 PXE Boot Support. If disabled IPV6 PXE boot option will not be created
Ipv6 HTTP Support	Enabled, Disabled	Enable Ipv6 HTTP Boot Support. If disabled IPV6 HTTP boot option will not be created
PXE boot wait time	1-5s	Wait time to press ESC key to abort the PXE boot
Media detect count	1-50	Number of times presence of media will be checked

6.8.11 CSM Configuration

Feature	Options	Description
CSM Support	Enabled Disabled	Enable/Disable CSM Support This module is able to emulate legacy **BIOS** environment and allow booting legacy operating systems or new operating systems which were installed without **UEFI** boot loader. If CSM is disabled, only EFI partitions can be booted. To disable CSM, first set Video Oprom to UEFI
GateA20 Active	Upon Request Always	UPON Request – GA20 can be disabled using BIOS services. Always – do not allow disabling GA20; this option is useful when any RT code is executed above 1MB

Feature	Options	Description
Interrupt 19 Response	Immediate Postponed	Bios reaction on INT19 trapping by Option Rom: Immediate – execute the trap right now Postponed – execute the trap during legacy boot
Boot option filter	UEFI and Legacy Legacy only UEFI only	This option controls what devices system can boot to.
Network	Do not launch UEFI only Legacy only	Controls the execution of UEFI and Legacy PXE OPROM. If enabled, the network controller appears as boot device and can be used to boot via PXE.
Storage	Do not launch UEFI only Legacy only	Controls the execution of UEFI and Legacy Storage OPROM
Video	Do not launch UEFI only Legacy only Legacy first UEFI first	Controls the execution of UEFI and Legacy Video OPROM. ⓘ **NOTICE: Legacy Video Bios is not supported by Intel for Apollo Lake. It should only be used for specific debugging situations.**
Other PCI device ROM	UEFI Oprom Legacy Oprom	For PCI devices other than Network, Mass storage or Video defines which Oprom to launch

6.8.12 NVMe Configuration

Feature	Options	Description
NVMe Device	Informative	Shows informations about initialised NVMe device (if connected)

6.8.13 SDIO Configuration

Feature	Options	Description
SDIO Device (eMMC, SD Card)	Informative	Shows the SDIO device found
SDIO Access Mode	Auto, ADMA, SDMA, PIO	Auto Option: Access SD device in DMA mode if controller supports it,otherwise in PIO mode.DMA Option: Access SD device in DMA mode.PIO Option: Access SD device in PIO mode.
MMC	Auto Floppy Forced FFD Hard Disk	Mass storage device emulation type. “AUTO” enumerates devices less than 530 MB as floppies. Forced FDD Option can be used to force HDD formatted drive to boot as FDD.

6.8.14 USB Configuration

Feature	Options	Description
Legacy USB support	Auto Enabled Disabled	Enables Legacy USB support. AUTO option disables legacy support if no USB devices are connected. DISABLE option will keep USB devices available only for EFI applications.
XHCI Hand-off	Enabled Disabled	This is a workaround for OSes without XHCI hand-off support. The XHCI ownership change should be claimed by XHCI driver.
USB Mass Storage Driver Support	Enabled Disabled	Enable/Disbale USB Mass Storage Driver Support.
USB transfer time-out	1 sec 5 sec 10 sec 20 sec	The time-out value for Control, Bulk, and Interrupt transfers.
Device reset time-out	10 sec 20 sec 30 sec 40 sec	USB mass storage device Start Unit command time-out.
Device power-up delay	Auto Manual	Maximum time the device will take before it properly reports itself to the Host Controller. 'Auto' uses default value: for a Root port it is 100 ms, for a Hub port the delay is taken from Hub descriptor.
Device power-up delay	Value 1-40	Delay range is 1…40 seconds, in one second increments.
USB Mass Storage Device (e.g USB Stick)	Auto Floppy Forced FDD Hard Disk CD-ROM	Select Mass storage device emulation type. Auto enumerates devices according to their media format. Optical drives are emulated as CDROM, drives with no media will be emulated according to a drive **Note:** This option is appears only if a USB storage device is connected.

6.8.15 Security Configuration

Feature	Options	Description
TXE HMRFPO	Enabled Disabled	Enable or disable TXE Host ME Region Flash Protection Override
TXE EOP Message	Enabled Disabled	Send EOP message before enter OS

6.8.16 SIO WB627/ SMSC 3114 Configuration

Feature	Options	Description
WB627 COM A-B:	Enabled Disabled	Enable or disable COM A-B on Winbond SIO
WB627 COM A-B Setting:	Auto I/O 3F8h, IRQ 4 I/O 3F8h, IRQ 3, 4, 5, 6, 7, 10, 11, 12 I/O 2F8h, IRQ 3, 4, 5, 6, 7, 10, 11, 12 I/O 3E8h, IRQ 3, 4, 5, 6, 7, 10, 11, 12 I/O 2E8h, IRQ 3, 4, 5, 6, 7, 10, 11, 12	Resource setting for COM A-B on Winbond SIO
WB627 LPT:	Disabled Enabled	Enable or disable LPT on Winbond SIO
Change Settings	Auto I/O 378h, IRQ 5, 7 I/O 278h, IRQ 5, 7	Resource setting for LPT A on Winbond SIO

Feature	Options	Description
LPT Mode:	SPP EPP 1.9 ECP ECP + EPP 1.9 Printer Mode EPP 1.7 ECP+EPP 1.7	Mode setting for LPT on Winbond SIO
WB627 PS/2 Controller	Disabled Enabled	Enable or disable the WB627 PS/2 controller.
WB627 HWM Interface	Disabled, Enabled	Enable or disable the hardware monitoring interface. If enabled, the base address 0x0290 will be used

Note: The above super IO menus will only appear if the SuperIO device is discovered on the carrier board.

6.8.17 EC Hardware Monitoring

Feature	Options	Description
CPU Fan Control	Manual, Temperature based	Define how the fan should be controlled: manually set to a fixed duty cycle, or temperature based auto control.
Fan Speed	Off, 25%, 50%, 75%, 100%	Setup the fan duty cycle for manual fan control.
By CPU sensor	Enabled, Disabled	If enabled, the cpu fan will be controlled by this temperature sensor.
By Board sensor	Enabled, Disabled	If enabled, the cpu fan will be controlled by this temperature sensor.
By Memory sensor	Enabled, Disabled	If enabled, the cpu fan will be controlled by this temperature sensor.
System Fan Control	Manual, Temperature based	Define how the fan should be controlled: manually set to a fixed duty cycle, or temperature based auto control.
Fan Speed	Off, 25%, 50%, 75%, 100%	Setup the fan duty cycle for manual fan control.
By CPU sensor	Enabled, Disabled	If enabled, the cpu fan will be controlled by this temperature sensor.
By Board sensor	Enabled, Disabled	If enabled, the cpu fan will be controlled by this temperature sensor.
By Memory sensor	Enabled, Disabled	If enabled, the cpu fan will be controlled by this temperature sensor.
CPU Throttling Control	Enabled, Disabled	Enable or disable the CPU throttling control.
By CPU sensor	Enabled, Disabled	If enabled, the CPU throttling can be triggered by this temperature sensor. ⓘ NOTE: This is the CPU temperature sensor from Boardcontroller which is near the CPU and not on die.
By Board sensor	Enabled, Disabled	If enabled, the CPU throttling can be triggered by this temperature sensor.

Feature	Options	Description
By Memory sensor	Enabled, Disabled	If enabled, the CPU throttling can be triggered by this temperature sensor.
CPU/Memory/Board Temperature Limit T1 [°C]	20, 25, 30, 35, 40, 45, 50, 55, 60 °C	Temperature threshold (in degrees Celsius) at which the fan should be set to maximum speed duty cycle. ⓘ NOTE: This option depends on selected temperature source (CPU/System/Board or a combination of these)
CPU/Memory/Board Temperature Limit T2 [°C]	40, 45, 50, 55, 60, 65, 70, 75, 80 °C	Temperature threshold (in degrees Celsius) at which the fan should be set to maximum speed duty cycle. ⓘ NOTE: This option depends on selected temperature source (CPU/System/Board or a combination of these)
CPU/Memory/Board Temperature Limit T3 [°C]	50, 55, 60, 65, 70, 75, 80, 85, 90, 95, 100 °C	Temperature threshold (in degrees Celsius) at which the fan should be set to maximum speed duty cycle. ⓘ NOTE: This option depends on selected temperature source (CPU/System/Board or a combination of these)
Critical Temperature Limit [°C]	60, 65, 70, 75, 80, 85, 90, 95, 100, 105, 110 °C	Temperature threshold (in degrees celsius) at which the CPU should be throttled.
CPU/Memory/Board Temperature Hysteresis	2°C, 4°C, 6°C, 8°C	The value (in degrees Celsius) that the temperature has to fall below a certain threshold before the next lower fan speed will be selected.

Detail explanation how fan control is working:

Detail explanation how fan control is working:

Up to 2 Fans are supported, either by manual mode with fixed duty cycles or by temperature based mode with dynamic duty cycles. The CPU fan is typically associated with the onboard CPU temperature sensor for automatic temperature control. The System fan is typically associated with one of the external temperature sensors and is set to manual mode per default.

In temperature based mode up to three different sources can be selected: CPU temperature, board temperature sensor and system temperature sensor.

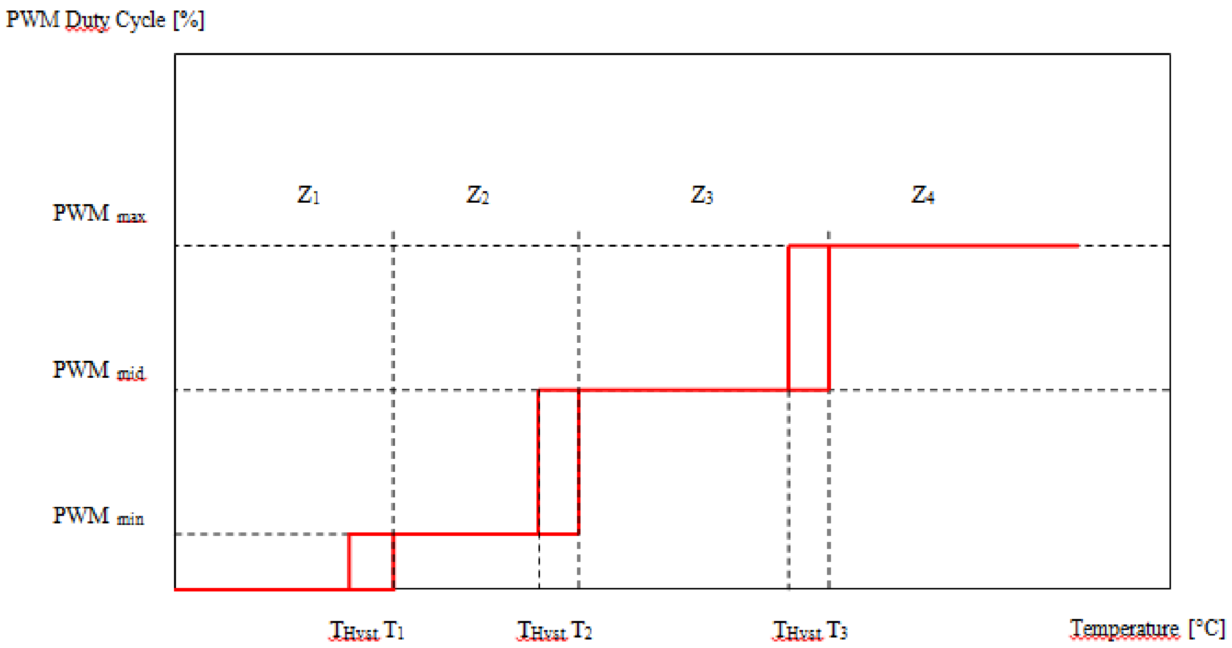
Temperature based mode controls fan within 4 temperature zones and fixed PWM duty cycles.

PWMmin 25%

PWMmid 50%

PWMmax 100%

The temperature zones can be selected by temperature limits (T1, T2, T3). The following diagram explains the temperature based fan control:



PWM min	Fan running with minimum speed (typically 25%)
PWM mid	Fan running with medium speed (typically 50%)
PWM max	Fan running with maximum speed (typically 100%)
Z1	Temperature zone T<T1, Fan stopped
Z2	Temperature zone T1<T<T2, Fan running with minimum speed
Z3	Temperature zone T2<T<T3, Fan running with medium speed
Z4	Temperature zone T2<T<T3, Fan running with maximum speed
T1	Minimum temperature limit starting Fan (selectable by SETUP)
T2	Temperature limit for medium Fan speed (selectable by SETUP)
T3	Temperature limit for maximum Fan speed (selectable by SETUP)
Thyst	Temperature hysteresis (selectable by SETUP)

Temperature Control with multiple Sensors

Fan control allows the association of any temperature sensor supported by embedded controller. This allows active fan control for more than one temperature. The supported temperature sensors are associated with the following onboard temperature areas:

- CPU temperature
- System temperature
- Memory temperature

Different temperature profiles for any temperature sensor can be selected in BIOS SETUP. If more than one temperature sensor is selected for fan control, the higher temperature exceeding the selected temperature limit (T1, T2, T3) gets precedence for fan regulation.

6.8.18 EC Features Configuration

Feature	Options	Description
Watchdog start on Boot	No Yes	Start the watchdog after BIOS POST if enabled
Startup Delay	1s 10s 30s 1min 5min	Select the initial delay value. This is an additional one-time delay before the standard timeout timer is started.
Event timeout	1s 10s 30s 1min 5min	Select the timeout value after which the watchdog will perform its timeout event action.
Event Action	Nothing WDOUT	Select the action that should be initiated after an event timeout occurs.
Reset Timeout	1s 10s 30s 1min 5min	Select the timeout value after which the watchdog will perform its reset action. This timeout will start to countdown after the event timeout expires.
Reset Action	Nothing Reset WDOUT WDOUT & Reset	Select the action that should take place after a reset timeout occurs.
POST Watchdog	Enabled, Disabled	Enable a watchdog during bios POST (before OS boot). ATTENTION: if this watchdog is configured with timeouts that are too agressive, the board might not be able to boot anymore!
Post Watchdog Timeout	20	The time in seconds that is available for the Bios to boot. When this time is exceed, the EC will try to recover the system througha reset or powercycle
Post Watchdog Action	Reset, Powercycle	Action to be performed after Post Watchdog time is execeed.

6.8.19 Module-specific Initialization

Feature	Options	Description
LAN Controller	Enabled,Disabled	Enable or disable the onboard LAN controller
ANX Controller	Enabled,Disabled	Enable or disable LVDS aNX1122 chip
TXE	Enabled,Disabled	TXE on/off
SD-Card / GPIO Selection	GPIO SD-Card	Select if ComExpress GPIO pins should be used as GPIOs or SD-Card interface
User I2C Support	GPIO-based, Controller based PCI mode	Select the type of user I2C support. GPIO based is for Windows and EAPI V4 or lower. Select Controller based for Linux and Windows with EAPI V5 or higher.
Set User I2C Speed	Standard Mode Fast Mode	Select User I2C Speed
LPSS User I2C Clock Gating Configuration	Enabled,Disabled	Enable/Disable LPSS User I2C Clock Gating
Shutdown Support	ATX Mode, AT Mode	ATX Mode means that the system will be turned off after shutdown. In AT mode, Windows will not automatically turn off the system, but instead show an informative string.
External SMBus Control	Enabled,Disabled	Enable/Disable External SMBus after POST

6.8.20 Onboard GPIO configuration

Feature	Options	Description
GPIO Configuration 0-3	Input Output Input & Output	GPIO Configuration
GPIO 0-3 Input Configuration (Interrupt Capabilities)	Rising Edge Falling Edge Both Edge	Define the condition under which an interrupt is generated
GPIO 0-7 Output Configuration (Default Value)	Output Low Output High	Define the default value for this GPIO.
GPIO 0-3 Input & Output Configuration (Default Value)	Output Low Output High Input	GPIO Configuration

ⓘ NOTE: On C10M-AL the GPIO 0-3 can be configured as Input and Output. GPO 3-7 can only be Output.

6.8.21 System Component

Feature	Options	Description
CRID Setting	CRID_0 – CRID_2; Disabled	Select the Revision ID reflected in PCI config space
OS Reset Select	Warm Reset, Cold Reset	Select the reset type in FACP table
DDR SSC	Enabled,Disabled	Enable DDR Spread Spectrum Clocking configuration
DDR SSC Selection Table	-0,1% - -0,5% ; 0%(No SCC)	DDR SSC Selection Table
DDR Clock Bending Selection Table	1,3%, 0,6%, 0,9%, 0%(No clock bending)	Choose for clock bending

Feature	Options	Description
HighSpeed SerialIO SSC	Enabled,Disabled	Enable HighSpeed SerialIO Spread Spectrum Clocking configuration
HighSpeed SerialIO SSC Selection Table	-0,1% - -0,5% ; 0%(No SCC)	Choose the item in SSC selection table for HighSpeed SerialIO spread spectrum

6.9 Chipset

Feature	Options	Description
Flat Panel Configuration	Submenu	Flat Panel Configuration
North Bridge	Submenu	North Bridge Settings
South Bridge	Submenu	South Bridge Settings
Uncore Configuration	Submenu	Uncore Configuration Settings
South Cluster Configuration	Submenu	South Cluster Configuration

6.9.1 Flat Panel Configuration

Feature	Options	Description
LVDS Panel Type	640x480 800x480 800x600 1024x768 1280x720 1280x800 1366x768	Select panel type. Only possible if external Eeprom is not connected or no EDID data found in non-volatile BIOS NVRAM.

Feature	Options	Description
LVDS Mapping	18bit, 24bit LDI 24bit FPDI	Select LVDS mapping type
LVDS Spread Spectrum	Disabled, (+-) 0,25% - 1,75%	Configure the spread spectrum for the LVDS interface.
LVDS Voltage Swing	100mV – 400mV	Configure the voltage swing for the LVDS interface.
Backlight Control	Submenu	Set Backlight settings

6.9.2 Backlight Control

Feature	Options	Description
Backlight_EN Control	Chipset, Always Off	Configures the backlight enable signal. This signal can either be controlled by chipset, or switched off.
Backlight_EN Polarity	Active Low, Active High	Define the polarity of the backlight enable signal.
PWM Control	EC, Chipset	EC means PWM will be controlled by the board controller. Chipset means PWM will be controlled by videobios.
PWM Polarity	Active Low, Active High	Backlight PWM signal polarity
PWM Brightness	0-100%	Select the initial brightness value of the flat panel
PWM Frequency	200HZ, 1KHz, 10KHz, 18KHz	Select backlight PWM frequency for brightness control

6.9.3 North Bridge

Feature	Options	Description
Max TOLUD	Dynamic 2GB 2.25 GB 2.5GB 2.75GB 3GB	Maximum Value of TOLUD.
Above 4GB MMIO BIOS assignment	Enabled, Disabled	Enable/Disable above 4GB MemoryMappedIO BIOS assignment This is disabled automatically when Aperture Size is set to 2048MB.
PCIE VGA Workaround	Enabled, Disabled	Enable it if your PCIe card cannot boot to DOS. This is for Test only

6.9.4 South Bridge

Feature	Options	Description
LPC Interface Configuration	Enabled, Disabled	Enable LPC interface, or disable it by setting all signals to GPIO mode. In GPIO mode, all pins will be inputs.
LPC CLKRUN# support	Enabled, Disabled	Enable LPC clockrun. If enabled, serial IRQ must be set to quiet mode. SIO and other LPC devices might cause problems if CLKRUN/quiet mode is enabled.
Serial IRQ Mode	Continuous, Quiet	Configure Serial IRQ Mode.
Real Time Option	RT Disabled, RT Enabled Agent ID1, RT Enabled Agent Disabled	Select Real-Time Enable and IDI Agent Real-Time Traffic Mask Bits

6.9.5 Uncore Configuration

Feature	Options	Description
GOP Driver	Enabled, Disabled	Enable GOP Driver will unload VBIOS; Disable it will load VBIOS
Intel Graphics Pei Display Peim	Enabled, Disabled	Enable/Disable Pei (Early) Display
GOP Brightness Level	0-255	Set GOP Brightness Level; Value ranges from 0-255
VBT Select	eDP-18 Bit Color LFP eDP-24 Bit Color LFP no LFP	Select VBT for GOP Driver
Integrated Graphics Device	Enabled, Disabled	Enable : Enable Integrated Graphics Device (IGD) when selected as the Primary Video Adaptor. Disable: Alwarys disable IGD
Primary Display	IGD, PCIe	Select which of IGD/PCI Graphics device should be Primary Display
RC6 (Render Standby)	Enabled, Disabled	Check to enable render standby support, RC6 should be enabled if S0ix is enabled. This item will be read only if S0ix is enabled
GTT Size	2MB, 4MB, 8MB	Select the GTT Size
Aperture Size	128 MB, 256MB, 512 MB	Select the Aperture Size
DVMT Pre-Allocated	64MB-512MB	Select DVMT 5.0 Pre-Allocated (Fixed) Graphics Memory size used by the Internal Graphics Device
DVMT Total Gfx Mem	128, 256, Max	Select DVMT5.0 Total Graphic Memory size used by the Internal Graphics Device
Cd Clock Frequency	144 MHz, 288MHz, 384 MHz, 576 MHz, 624MHz	Select the highest Cd Clock frequency supported by the platform
GT PM Support	Enabled, Disabled	Enable/Disable GT PM Support
PAVP Enable	Enabled, Disabled	Enable/Disable PAVP
Memory Scrambler	Enabled, Disabled	Enable/Disable Memory Scrambler support.

Feature	Options	Description
Minimum Refresh Rate of 2x		Enabling this will double the DRAM refresh rate, at the cost of memory bandwidth. Required for iTemp memory support and countering the rowhammer attack.

6.9.6 South Cluster Configuration

Feature	Options	Description
HD Audio Configuration	Submenu	HD-Audio Configuration Settings
LPSS Configuration	Submenu	LPSS Configuration Settings
PCI Express Configuration	Submenu	PCI Express Configuration
SATA Drives	Submenu	SATA Drives
SCC Configuration	Submenu	SCC Configuration Settings
USB Configuration	Submenu	USB Configuration
Miscellaneous Configuration	Submenu	Enable/Disable Misc. Features

6.9.7 HD Audio Configuration

Feature	Options	Description
HD-Audio Support	Enabled Disabled	Control Detection of the Azalia device. Disabled = Azalia will be unconditionally disabled Enabled = Azalia will be unconditionally Enabled Auto = Azalia will be enabled if present, disabled otherwise.
HD-Audio DSP	Enabled Disabled	Enable/Disable HD-Audio DSP
HD-Audio PME	Enabled Disabled	Enables PME wake of HD Audio controller during POST.

6.9.8 LPSS Configuration

Feature	Options	Description
CAM1 I2C Controller	PCI Mode Disabled	Enable/Disable the CAM1 I2C Controller
Set CAM1 I2C Speed	Standard Mode Fast Mode Fast Plus Mode High Speed Mode	Select CAM1 I2C Speed
LPSS HSUART #1 Support (D24:F0)	Disabled, PCI Mode	Enable/Disable LPSS HSUART #1 Support
LPSS HSUART #2 Support (D24:F1)	Disabled, PCI Mode	Enable/Disable LPSS HSUART #2 Support
LPSS SPI #1 Support (D25:F0)	Disabled, PCI Mode	Enable/Disable LPSS SPI #1 Support
LPSS IOSF PMCTL S0ix Enable	Enabled Enabled	Enable LPSS IOSF Bridge PMCTL Register S0ix Bits

Feature	Options	Description
	Disabled	
LPSS CAM1 I2C Clock Gating Configuration	Enabled Disabled	Enable/Disable LPSS CAM1 I2C Clock Gating
LPSS HSUART #1 Clock Gating Configuration	Enabled Disabled	Enable/Disable LPSS HSUART #1 Clock Gating
LPSS HSUART #2 Clock Gating Configuration	Enabled Disabled	Enable/Disable LPSS HSUART #2 Clock Gating
LPSS SPI #1 Clock Gating Configuration	Enabled Disabled	Enable/Disable LPSS SPI #1 Clock Gating

6.9.9 PCI Express Configuration

Feature	Options	Description
PCI Express Clock Gating	Enabled, Disabled, Auto	Control the PCI Express Root Port. Auto: To disable unused root por automatically for most optimum power savings.
Port8xh Decode Port	Enabled, Disabled	Select which PCI Express Root Port should claim accesses to I/O port 8xh
Peer Memory Write Enable	Enabled, Disabled	Peer Memory write Enable/Disable
Compliance Mode	Enabled, Disabled	Compliance Mode Enable/Disable
PCIE Express Root Port A 0-3 and Port B 1 (LAN)	Submenu	Configure PCIE Express Root Port Settings

6.9.10 PCIE Express Root Port A 0-3 and B1 (LAN)

Feature	Options	Description
PCI Express Root Port x	Enabled Disabled	Control the PCI Express Root Port.
ASPM	Enabled Disabled	PCI Express Active State Power Management settings.
L1 Substances	Disabled L1.1 L1.2 L1.1 & L1.2	PCI Express L1 Substates settings.
ACS	Enabled Disabled	Enable/Disable Access Control Services Extended Capability
URR	Enabled Disabled	PCI Express Unsupported Request Reporting Enable/Disable.
FER	Enabled Disabled	PCI Express Device Fatal Error Reporting Enable/Disable.
NFER	Enabled Disabled	PCI Express Device Non-Fatal Error Reporting Enable/Disable.
CER	Enabled Disabled	PCI Express Device Correctable Error Reporting Enable/Disable
CTO	Default Setting 16-55 ms 65-210 ms 260-900 ms 1-3.5 s Disabled	PCI Express Completion Timer TO Enable/Disable.
SEFE	Enabled Disabled	Root PCI Express System Error on Fatal Error Enable/Disable.
SENFE	Enabled Disabled	Enable or disable Root PCI Express System Error on Non-Fatal Error

Feature	Options	Description
SECE	Enabled Disabled	Root PCI Express System Error on Correctable Error Enable/Disable.
PME SCI	Enabled Disabled	PCI Express PME SCI Enable/Disable.
Hot Plug	Enabled Disabled	PCI Express Hot Plug Enable/Disable
PCIe Speed	Auto, GEN1, GEN2	Configure PCIe Speed. CHV A1 always with Gen1 Speed.
Transmitter Half Swing	Enabled Disabled	Transmitter Half Swing Enable/Disable.
PCH PCIE LTR	Enabled Disabled	PCH PCIE Latency Reporting Enable/Disable
Snoop Latency Override	Disabled Manual Auto	Snoop Latency Override for PCH PCIE. Disabled: Disable override. Manual: Manually enter override values. Auto (default): Maintain default BIOS flow.
Non Snoop Latency Override	Disabled Manual Auto	Non Snoop Latency Override for PCH PCIE. Disabled: Disable override. Manual: Manually enter override values. Auto (default): Maintain default BIOS flow.
PCIE LTR Lock	Enabled Disabled	PCIE LTR Configuration Lock
PCIe Selectable De-emphasis	Enabled Disabled	When the Link is operating at 5.0 GT/s speed, this bit selects the level of de-emphasis for an Upstream component. 1b -3.5 dB 0b -6 dB

6.9.11 SATA Drives

Feature	Options	Description
Chipset SATA	Enable, Disable	Enables or Disables the Chipset SATA Controller. The Chipset SATA controller supports 2 SATA ports (up to 6Gb/s supported per port)
SATA Controller Speed	Default, Gen1-3	Limit the maximum speed of the SATA controller
SATA Test Mode	Enable, Disable	Test Mode Enable/Disable
Aggressive LPM Support	Enable, Disable	Enable PCH to aggressively enter link power state.
Port x	Enable, Disable	Enable or Disable SATA Port
SATA Port x Hot Plug	Enable, Disable	If enabled, SATA port will be reported as Hot Plug capable.
Spin Up Device	Enable, Disable	If enabled for any of ports Staggerred Spin Up will be performed and only the drives which have this option enabled will spin up at boot. Otherwise all drives spin up at boot

6.9.12 SCC Configuration

Feature	Options	Description
SCC SD Card Support (D27:F0)	Enable, Disable	Enable/Disable SCC SD Card Support
SD Card Max Speed	SDR104 + SDR50 + DDR50 SDR104 + SDR50 SDR104 + DDR50 SDR104 SDR50 + DDR50 SDR50 DDR50	Select the SD Card max Speed allowed. DDR50: 50MHz clock SDR50: 100MHz clock SDR104: 200MHz clock

Feature	Options	Description
SCC eMMC Support (D28:F0)	Enable, Disable	Enable/Disable SCC eMMC Support
eMMC Max Speed	DDR50, HS200, HS400	Select the eMMC max Speed allowed.
SCC SDIO Support (D30:F0)	Enable, Disable	Enable/Disable SCC SDIO Support

6.9.13 USB Configuration

Feature	Options	Description
XHCI Pre-Boot Driver	Enabled Disabled	Enable/Disable XHCI Pre-Boot Driver support.
USB 2 Port 0-7	Enabled Disabled	Enable/Disable USB port. Once disabled, any USB devices plug into the connector will not be detected by BIOS or OS
USB 3 Port 0-1	Enabled Disabled	Enable/Disable USB port. Once disabled, any USB devices plug into the connector will not be detected by BIOS or OS
XDCI Support	Disabled PCI Mode	Enable/Disable XDCI
XHCI Disable Compliance Mode	True, False	Options to disable XHCI Link Compliance Mode. Default is FALSE to not disable Compliance Mode. Set TRUE to disable Compliance Mode
USB HW MODE AFE Comparators	Enabled Disabled	Enable/Disable USB HW MODE AFE Comparators

6.9.14 Miscellaneous Configuration

Feature	Options	Description
State After G3	S0 State, S5 State	Specify what state to go to when power is re-applied after a power failure (G3 state). S0 State: System will boot directly as soon as power applied. S5 State: System keeps in power-off state until power button is pressed.
Board Clock Spread Spectrum	Enabled Disabled	Enable Clock Chip's Spread Spectrum feature
Wake On Lan	Enabled Disabled	Enable or Disable the Wake on Lan
BIOS Lock	Enabled Disabled	Enable/Disable the SC BIOS Lock Enable feature. Required to be enabled to ensure SMM protection of flash.
RTC Lock	Enabled Disabled	Enable will lock bytes 38h-3Fh in the lower/upper 128-byte bank of RTC RAM
Flash Protection Range Registers (FPRR)	Enabled Disabled	Enable Flash Protection Range Registers

6.10 Security

Feature	Options	Description
Administrator Password	Set Password	Set Setup Administrator Password
User Password	Set Password	Set User Password
HDDSecurity Configuration	Set Password	Set HDD Password
Secure Boot Menu	Submenu	Enter Secure Boot Menu

Note: If ONLY the Administrator's password is set, then this only limits access to Setup and is only prompted for when entering Setup.

If ONLY the User's password is set, then this is a power on password and must be entered to boot or enter Setup. In Setup the User will have Administrator rights.

6.10.1 Secure Boot

Feature	Options	Description
Secure Boot	Enabled, Disabled	Secure Boot activated when Platform Key(PK) is enrolled, System mode is User/Deployed, and CSM function is disabled ⓘ NOTE: If Secure Boot will be enabled, System Bios is immediately configured without CSM.
Secure Boot Customization	Standard, Custom	Secure Boot Mode - Custom & Standard, Set UEFI Secure Boot Mode to STANDARD mode or CUSTOM mode, this change is effect after save. And after reset, the mode will return to STANDARD mode
Restore Factory Keys	Install factory defaults Yes or No	Force System to User Mode. Configure NVRAM to contain OEM-defined factory default Secure Boot keys

Feature	Options	Description
Key Management	Submenu	Enables expert users to modify Secure Boot Policy variables without full authentication

6.10.2 Key Management

Feature	Options	Description
Factory Key Provision	Enabled, Disabled	Provision factory default keys on next re-boot only when System in Setup Mode
Restore Factory Keys	Restore Factory Default Yes or No	Force System to User Mode. Configure NVRAM to contain OEM-defined factory default Secure Boot keys
Enroll Efi Image	“Enter”	Allow the image to run in Secure Boot mode. Enroll SHA256 Hash certificate of a PE image into Authorized Signature Database (db)
Restore DB defaults	“Enter”	Restore DB variable to factory defaults
Platform Key (PK)	“Enter”	Enroll Factory Default or load certificates from a file: 1. Public Key Certificate in: a) EFI_SIGNATURE_LIST b) EFI_CERT_X509 (DER encoded) c) EFI_CERT_RSA2048 (bin) d) EFI_CERT_SHA256, 385, 512 2. Authenticated UEFI Variable 3. EFI PE/COFF Image (SHA256) Key Source: Factory, External, Mixed

Feature	Options	Description
Key Exchange Keys	Update Append	Enroll Factory Default or load certificates from a file: 1. Public Key Certificate in: a) EFI_SIGNATURE_LIST b) EFI_CERT_X509 (DER encoded) c) EFI_CERT_RSA2048 (bin) d) EFI_CERT_SHA256, 385, 512 2. Authenticated UEFI Variable 3. EFI PE/COFF Image (SHA256) Key Source: Factory, External, Mixed
Authorized Signatures	Update Append	Enroll Factory Default or load certificates from a file: 1. Public Key Certificate in: a) EFI_SIGNATURE_LIST b) EFI_CERT_X509 (DER encoded) c) EFI_CERT_RSA2048 (bin) d) EFI_CERT_SHA256, 385, 512 2. Authenticated UEFI Variable 3. EFI PE/COFF Image (SHA256) Key Source: Factory, External, Mixed
Forbidden Signatures	Update Append	Enroll Factory Default or load certificates from a file: 1. Public Key Certificate in: a) EFI_SIGNATURE_LIST b) EFI_CERT_X509 (DER encoded) c) EFI_CERT_RSA2048 (bin) d) EFI_CERT_SHA256, 385, 512 2. Authenticated UEFI Variable 3. EFI PE/COFF Image (SHA256) Key Source: Factory, External, Mixed

Feature	Options	Description
Authorized TimeStamps	Update Append	Enroll Factory Default or load certificates from a file: 1. Public Key Certificate in: a) EFI_SIGNATURE_LIST b) EFI_CERT_X509 (DER encoded) c) EFI_CERT_RSA2048 (bin) d) EFI_CERT_SHA256, 385, 512 2. Authenticated UEFI Variable 3. EFI PE/COFF Image (SHA256) Key Source: Factory, External, Mixed
OsRecovery Signatures	Update Append	Enroll Factory Default or load certificates from a file: 1. Public Key Certificate in: a) EFI_SIGNATURE_LIST b) EFI_CERT_X509 (DER encoded) c) EFI_CERT_RSA2048 (bin) d) EFI_CERT_SHA256, 385, 512 2. Authenticated UEFI Variable 3. EFI PE/COFF Image (SHA256) Key Source: Factory, External, Mixed

6.11 Boot

Feature	Options	Description
Setup Prompt Timeout	1-65535sec	Number of seconds to wait for setup activation key. 65535(0xFFFF) means wait forever.
Bootup NumLock State	On Off	Select the keyboard NumLock state
Quiet Boot	Enabled Disabled	Enables/Disables Quiet Boot option
Boot Priority 1	SATA Port 0/1, USB 2.0 Port 0-7, USB 3.0 Port 0-1, eMMC, SD Card, LAN, UEFI LAN, External Devices	Define which boot device should have the highest boot priority Note: If the connected device has a legacy and uefi boot path, uefi will be the higher priority. This can be avoided by filtering UEFI Boot out
Boot Priority 2	SATA Port 0/1, USB 2.0 Port 0-7, USB 3.0 Port 0-1 eMMC, SD Card, LAN, UEFI LAN, External Devices	Define which boot device should have the second highest boot priority
Boot Priority 3	SATA Port 0/1, USB 2.0 Port 0-7, USB 3.0 Port 0-1 eMMC, SD Card, LAN, UEFI LAN, External Devices	Define which boot device should have the third highest boot priority
Boot Priority 4	SATA Port 0/1, USB 2.0 Port 0-7, USB 3.0 Port 0-1 eMMC, SD Card, LAN, UEFI LAN, External Devices	Define which boot device should have the fourth highest boot priority
Allow other devices	Yes, No	If set to no, only devices defined in the advanced boot device selection items are allowed to boot

Feature	Options	Description
Boot option filter	UEFI and Legacy, Legacy only, UEFI only	This option controls Legacy/UEFI ROMs priority. If set to Legacy only, then no UEFI Device will be bootable. If set to UEFI only, UEFI devices will be bootable. ⓘ **NOTICE** : Legacy boot is included but will no longer be supported by Intel. Use legacy boot for demo/testing with these settings: CSM Support [Enabled] Boot Filter [UEFI / Lagacy] Video [Legacy]
Boot Option #1…	Device x	Sets the system boot order. Please note that UEFI boot entries will always have the highest priority. This list will be updated during next boot depending on the settings in the Advanced Boot Device Selection. Note: The number of available Boot options is dependent on the devices which are connected. This windows shows the actual configured boot priority list which is set in the Boot Priority options above Note: By pressing [F10] during POST system will display a Boot Menu for directly booting a selected device.
Fast Boot	Enabled Disabled	Enables/Disables boot with initialization of a minimal set of devices required to launch active boot option. Has no effect for BBS boot options. For more information see also technotes in chapter 7
SATA Support	Last Boot HDD Only All Sata Devices	SATA Support
VGA Support	Auto, EFI Driver	If Auto, only install legacy Oprom with legacy OS and logo would not be shown during post. EFI driver will still be installed with EFI OS
USB Support	Disabled, Full Initial, Partial Initial	If Disabled, all USB devices will NOT be available until after OS boot. If Partial Initial, USB Mass Storage and specific USB port/device will NOT be available before OS boot. If Full Initial, all

Feature	Options	Description
		USB devices will be available in OS and Post. Note: If disabled, entering Setup will only be possible by performing a System Reset (with Reset Button) during OS Boot, or by clearing CMOS with the Clear CMOS Jumper.
PS2 Devices Support	Enabled, Disabled	If disabled, PS2 devices will be skipped
Network Stack Driver Support	Enabled, Disabled	If disabled, Network Stack driver will be skipped
Redirection Support	Enabled, Disabled	If disabled, Redirection function will be disabled
New Boot Option Policy	Default, Place First, Place Last	Controls the placement of newly detected UEFI boot options

6.12 Save & Exit

The following sections describe each of the options in this menu.

Save Changes and Exit

After making changes in the setup menus, always select "Exit Saving Changes". This procedure stores the selections displayed in the menus in a flash. The next time you boot your computer, the BIOS configures your system according to the setup selections stored in flash.

If you attempt to exit without saving, the program asks if you want to save before exiting. During boot-up, the Aptio BIOS attempts to load the values saved in flash. If those values cause the system boot to fail, reboot and press [ESC] or [DEL] to enter Setup. In Setup, you can restore the Default Values (as described below) or try to change the selections that caused the boot to fail.

Discard Changes and Exit

Exit system setup without saving any changes.

Save Changes and Reset

When you have completed the system configuration changes, select this option to save the changes and reboot the system, so the new system configuration parameters can take effect.

Discard Changes and Reset

Select this option to quit Aptio™ TSE without making any modifications to the system configuration

Save Changes

Selecting "Save Options" saves all the selections without exiting Setup. You can return to the other menus if you want to review and change your selections.

Discard Changes

Discard changes made so far to any of the setup options

Restore Defaults

Restore/load default values for all the setup options

Restore User Defaults

Restore the User defaults to all the setup options.

Save as User Defaults

Save changes done so far as User defaults.

Boot Override

It will display all the available boot options from the Boot Option List. The user can select any of the options to select to the particular device and boot directly from it.

Launch EFI Shell from filesystem device

Attempts to Launch EFI Shell application (Shellx64.efi) from one of the available filesystem devices.

WARNING! This function will still work even if mass storage devices are not registered into the boot device list via MSC BIOS Configuration tool MBconf tool. For example, only Harddisk is registered as possible boot device and a USB Stick with an EFI shell is plugged, the shell can still be executed (from the USB Stick) with this option.

Bios and Firmware Update

6.13 Setup Controlled Update

Within BIOS Setup main menu a submenu “MSC Firmware Update” is integrated to define settings for BIOS updates and initially trigger the update

Control flags define the section of FLASH which needs to be updated (BIOS only, complete FLASH, partial BIOS sections, etc.) and other options like screen output, preserving DMI data, etc.
The update file (a complete SPI firmware image) has to be stored at a fixed location within the file system on a mass storage device. BIOS loads the file into RAM, performs optional security checks and finally programs the data to the BIOS FLASH according to supplied control flags.

Update from Local Block Device:

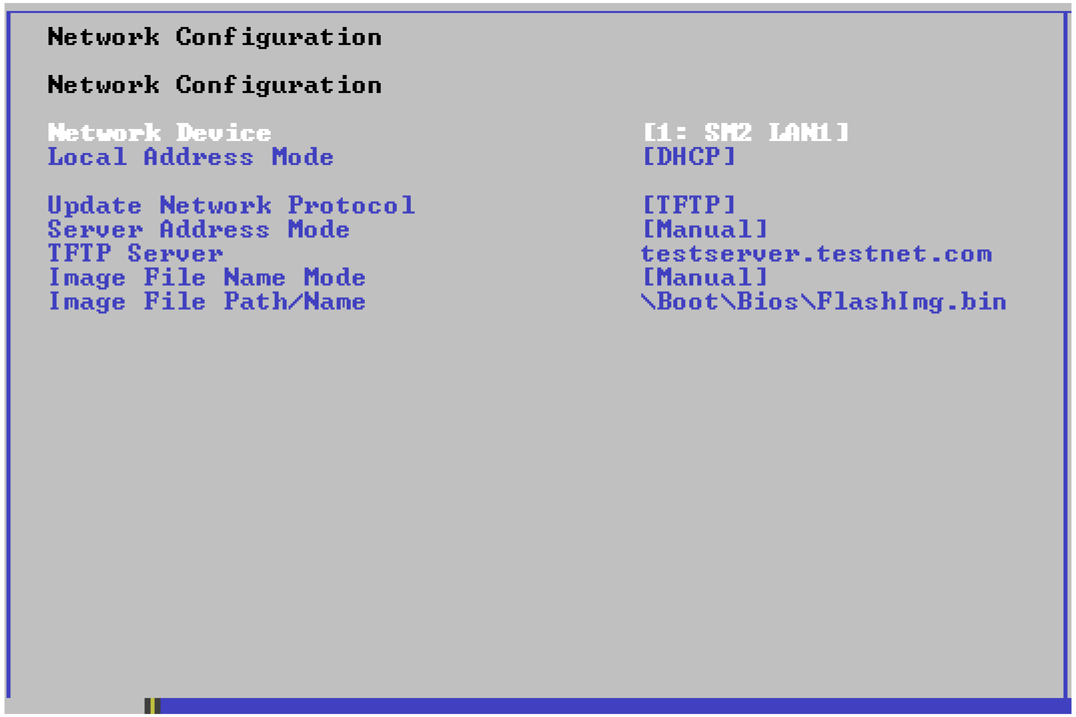
Supported mass storage devices (platform dependent): USB, SATA, eMMC
Supported file systems (platform dependent): FAT, FAT32, EXT3, EXT4, NTFS
Image location within file system: /Recovery/FlashImg.bin

- To start the update make sure that the medium with the correct Bios stored is connected and Update Source is set to “Local Block Devices”.
- In Bios section Main/MSC Firmware Update configure control flags as needed. Then enter “Start firmware Update”.
- After Bios update is done system will reboot.

Update from Network:

To Update via Network set the Update source to “Network” and configure the network settings. Below is an example screenshot.

The Image must be located on a TFTP Share. Enter the Server name and the path to the image. Press ESC to return to firmware update page, then press “Start firmware update” with configured firmware update features to start the. Make sure your network cable is attached in the selected network device. After a reset the update procedure will begin. First the link is checked and the when the bios update image is found on TFTP share, the image will be downloaded and the Bios will be updated.



```
Network Configuration

Network Configuration

Network Device                         [1: SM2 LAN1]
Local Address Mode                     [DHCP]

Update Network Protocol                [TFTP]
Server Address Mode                    [Manual]
TFTP Server                            testserver.testnet.com
Image File Name Mode                   [Manual]
Image File Path/Name                   \Boot\Bios\FlashImg.bin
```

It is also possible to initiate the network update with AutoFlash from EFI, Windows or Linux by adding a config file with all network parameters.

Here is an example of a simple .txt file which contains the network configuration data, ts is loaded by Autflash with the switches : -net –nc [Filename]

e.g AutoFlash.efi –u –e –net –fc configfile.txt

Network Interface : 0

Config Mode : DHCP

Network Protocol : TFTP

Server Address Mode: static

Server Name : testserver.testnet.com

File Name Mode : manual

Image File Name : \Boot\Bios\FlashImg.bin

6.14 Bios Update from EFI Shell

BIOS Update - Batch Mode

1. Create an EFI shell bootable USB stick by copying the shell binary to target directory \EFI\boot\bootx64.efi
2. Copy the update file to \Recovery\FlashImg.bin
3. Copy the update script to root directory (if required add -e to AutoFLASH.efi commandline)
4. Copy update tool to root directory \AutoFLASH.EFI
5. Make sure, USB stick is at first position of boot device list
6. Reboot system to EFI shell and execute update script and follow instructions on screen
7. Do NOT switch off power and wait until BIOS update has completed

6.15 Bios Update from Linux

It is also possible to trigger the update from Linux.

Make sure the Image location is within file system: /Recovery/FlashImg.bin and the device is inserted as described in 6.13.

To start the update from Linux, run the AutoFLASH tool as root (and probably set the permission for the file with “chmod 775 AutoFLASH”):

./AutoFLASH –u

Then reboot system. The update will start automatically.

6.16 Bios Update from Windows

And it is also possible to trigger the update from Windows which is booted in UEFI-Mode.

Make sure the Image location is within file system: /Recovery/FlashImg.bin and the device is inserted as described in 6.13.

To start the update from Linux, run the AutoFLASH tool as Administrator from your Windows Console with <Autoflash.exe –u>

Then reboot system. The update will start automatically.

6.17 Blind Restoration of Bios default settings (no display available)

1. Power up the System
2. Repeatedly press [DEL] for several seconds
3. Press [F3] for default settings or [F2] for previous values.
4. Press [Enter]
5. Press [F4]
6. Press [Enter]
7. System will restart
8. Alternatively it is possible to restore Bios defaults by shorting two pins on the module. See chapter 6.18.

6.18 Bios Recovery

If a Bios update will be interrupted (e.g due to power loss) and the update has not been finished, it can happen that the system will not boot. In this case it is possible to restore the Bios with the following method:

1. Prepare the SPI Image (flashimg.bin) as described in section 6.13
2. Power on the system.
3. Bios will search for the file and if found a Bios recovery will be started.
4. After Bios recovery is finished the system will perform a powercycle and the system should boot normal again without the recovery medium

It is also possible to initialise the bios recovery by shorting the recovery pins on the module as described in chapter 3.1

ⓘ NOTICE: During Bios recovery there is no video output. Users have to wait until power cycle will be performed. So it is recommended to wait some minutes until power cycle is performed.

6.19 Trusted Update

General Information

The Trusted Update feature is a combination of bios-based features and external tools which provides security for the bios update process. The aim is to secure the bios against attacks that try to change the bios flash content, while still allowing trusted parties to update the bios.

The following items are part of Trusted Update:

Flash write-protection

The bios will write-protect its own flash to prevent malicious applications from changing the bios code. This write-protection can only be disabled by a global reset, so flash writes can only be done by the bios code itself.

Hash-based checksum checks for bios images

Bios images include a hash-based checksum to safeguard against file and/or memory corruption. This hash will be checked before programming a new bios.

Bios update security with cryptographic signatures

As an optional enhancement, customers can patch a bios with their own public key. If a bios includes a public key for trusted updates, the bios will only accept bios update images signed with the corresponding private key.

Availability of easy to use tools

Bios images can still be edited with the MSC bios editor, as the editor will automatically ensure that your bios checksum is updated. If customer keys are provided, the bios editor will be able to patch the public key into the bios and create a signature for the image.

Required Tools for configuring Trusted Update:

- MSC Bios Editor (version V2.30 or later)

One of the following for creating the required keys:

- MakeCert.exe (provided by Microsoft WinDDK or Platform SDK)
- OpenSSL (available from https://www.openssl.org)

You will need a bios image which supports the Trusted Update feature. You can check for Trusted Update support in a variety of ways:

- With a live system, go into setup and enter the “Firmware Update” submenu. If the last line starts with “Trusted Update”, it is supported in this bios version.
- When you load a bios image into the MSC bios editor (V2.30 or later), bios images with support for Trusted Update will show a tab called “Trusted Update”.
- Ask your MSC contact if the bios for your platform supports this feature.

Key Creation

The bios and the editor will use the same key file format as the Microsoft signing tools (*.cer for public key certificates, *.pfx for private keys). Creating a key pair can be done with the tools provided by Microsoft or OpenSSL.Current bios implementations can work with keys that use hash algorithms SHA256/SHA384/SHA512, and RSA as cryptographic algorithm (key length of 2048 and 4096 bits).

The following examples create RSA keys with a length of 2048 bits, and set hash usage to SHA256.

Key Creation with MakeCert

```
MakeCert -r -a sha256 -len 2048 -n "CN=<certificate name>" -sv key.pvk key.cer
```

```
pvk2pfx -pvk key.pvk -spc key.cer -pfx key.pfx -pi <password>
```

Since Trusted Update uses the same format as the Microsoft tools, those files can be used directly. The important files are the private key file “key.pfx” and the public key certificate “key.cer”.

Key Creation with OpenSSL

```
openssl req -x509 -sha256 -nodes -days 365 -newkey rsa:2048 -keyout key.key -out key.crt
```

```
openssl x509 -in key.crt -outform der -out key.cer
```

```
openssl pkcs12 -export -out key.pfx -inkey key.key -in key.crt
```

OpenSSL generates keys in a different format, therefore some conversion must be done before those keys can be used for Trusted Update. However, all required conversion can be done with the openssl tool, as seen above. The important files are the private key file “key.pfx” and the public key certificate “key.cer”.

Trusted Update key usage

MakeCert or OpenSSL will prompt you for a password when generating a private key. This password is used to protect the access to the private key. Whenever the private key is used (i.e. pvk2pfx or bios editor), this password must be provided.

Self-signed certificates will be used, as it is not possible for the bios to check key hierarchies.

The “valid date” certificate entry will be ignored by the bios, as there is no reliable time source available during bios execution.

MSC Bios Editor Usage

Standard usage for creating a bios image with active signature verification:

1. Open up the bios editor and load your bios image file.

2. Click on the “Trusted Update” tab. If there is no “Trusted Update” tab, the currently loaded bios image does not support Trusted Update yet.

3. Use the public key certificate “Add…” button to add your public key file to the bios. This public key will be used for checking bios image signatures when this bios is running. Unsigned bios updates are only possible if this field is left blank. If there is a public key already present in the bios image, the text on the button changes to “Replace…”.

4. If you need to create a signature for this bios image, check the “Sign Image” checkbox. To create a signature, the editor will need access to the private key. Use the personal information exchange file “Load…” button to point to your private key *.pfx file, and enter the required password into the boxes below.

5. Now save your bios image, and the bios file will be updated with the provided public key, and a signature for Trusted Update will be generated and added to the bios image.

Example Usage: Switching from unsigned to signed updates

If your currently running bios has Trusted Update not enable yet, you only need to set a public key certificate. Since the currently running bios does not include a public key for signature verification, it is not necessary to generate a signature for the first bios update. However, generating a signature will not cause any problems.

Example Usage: Switching from signed to unsigned updates

It is possible to switch back to unsigned updates by generating a bios image which includes a valid signature, but no public key. The signature ensures that the image can be updated by a bios which only accepts signed images, while the missing public key means that further bios updates do not require a signature. You can remove an existing key from a bios image with the “Remove…” button on the “public key certificate” line.

6.20 Jumpers

There are two jumpers available on the module:

Clear Backup EEPROM: By shorting the pins of this jumper during boot, the values of the Backup EEPROM and the values of the NV-ROM are invalidated, thus forcing the board to start up with default values.

BIOS Recovery: By shorting the pins of this jumper during boot the system is forced into crisis recovery mode.

For more information see chapter 3.1

6.21 Post Codes

For Post Code information please visit the Avnet Embedded Support Website or contact Avnet Embedded /MSC Technical Support:

Email: support.boards@avnet.eu

Phone: +49 8165 906-200

7 Technotes

.

EIST (Enhanced Intel® Speed Step)

This allows the processor to meet the instantaneous performance needs of the operation being performed, while minimizing power draw and heat dissipation. Processor clock will be at its minimum possible frequency when in IDLE. When performing CPU loads, it will change its frequency up to its maximum frequency.

Note: If EIST is disabled in setup, the CPU will run at its maximum speed. Turbo Boost Technology won’t be available.

Turbo Boost Technology 2.0

Intel® Turbo Boost is a technology that enables the processor to run above its base operating frequency via dynamic control of the CPU's "clock rate". It is activated when the operating system requests the highest performance state of the processor. The increased clock rate is limited by the processor's power, current and thermal limits, as well as the number of cores currently in use and the maximum frequency of the active cores.

For more information about Intel® Turbo Boost 2 Technology visit the Intel® website.

Note: Turbo Boost will only work if EIST is enabled.

Reference: http://en.wikipedia.org/wiki/Intel_Turbo_Boost

ASPM (Active State Power Management)

Active State Power Management or ASPM is a power management protocol used to manage PCI Express-based serial link devices as links become less active over time.

As serial-based PCIe bus devices, such as IEEE1394 (FireWire), become less active, it is possible for the computer's power management system to take the opportunity to reduce overall power consumption by placing the link PHY into a low-power mode and instructing other devices on the link to follow suit.

Reference: http://en.wikipedia.org/wiki/Active_State_Power_Management

Intel® VT and VT-d

Increasing manageability, security, and flexibility in IT environments, virtualization technologies like hardware-assisted Intel® Virtualization Technology (Intel® VT) combined with software-based virtualization solutions provide maximum system utilization by consolidating multiple environments into a single server or PC. By abstracting the software away from the underlying hardware, a world of new usage models opens up that reduce costs, increase management efficiency, strengthen security, while making your computing infrastructure more resilient in the event of a disaster.

For more information about the technology please visit: http://www.intel.com/technology/virtualization/

VT-d supports the remapping of I/O DMA transfers and device-generated interrupts. The architecture of VT-d provides the flexibility to support multiple usage models that may run un-modified, special-purpose, or "virtualization aware" guest OSs. The VT-d hardware capabilities for I/O virtualization complement the existing Intel® VT capability to virtualize processor and memory resources. Together, this roadmap of VT technologies offers a complete solution to provide full hardware support for the virtualization of Intel® platforms.

Reference: http://ark.intel.com/VTList.aspx

http://www.intel.com/technology/itj/2006/v10i3/2-io/7-conclusion.htm

Fast Boot

Fast Boot supported by Aptio provides faster boot time by learning the system configuration on the first boot. On the Next boot system boots faster because the bios will only use the best boot path from the first OS boot. It configures only devices needed for the OS to boot. It adapts when system changes.

Note: Enabling Fast Boot makes only sense with Windows 8 and above. The speedup is minimal and only recommended if complete system configuration is tested with Fast Boot enabled.

Trusted Platform Module (TPM)

A TPM is a cryptoprocessor that can store cryptographic keys that protect information.

The Trusted Platform Module offers facilities for the secure generation of cryptographic keys, and limitation of their use, in addition to a hardware pseudo-random number generator. It also includes capabilities such as remote attestation and sealed storage.

"Remote attestation" creates a nearly unforgettable hash-key summary of the hardware and software configuration. The program encrypting the data determines the extent of the summary of the software. This allows a third party to verify that the software has not been changed.

"Binding" encrypts data using the TPM endorsement key, a unique RSA key burned into the chip during its production, or another trusted key descended from it.

"Sealing" encrypts data in similar manner to binding, but in addition specifies a state in which the TPM must be in order for the data to be decrypted (unsealed).

Software can use a Trusted Platform Module to authenticate hardware devices. Since each TPM chip has a unique and secret RSA key burned in as it is produced, it is capable of performing platform authentication. For example, it can be used to verify that a system seeking access is the expected system.

Reference: http://en.wikipedia.org/wiki/Trusted_Platform_Module

TXT (Trusted Execution Technology)

Due to the complexity of this feature, please visit http://www.intel.com/content/dam/www/public/us/en/documents/white-papers/trusted-execution-technology-security-paper.pdf

Note: To use this feature VT, Vt-d, SMX and TPM must be enabled.

8 EAPI

The "Embedded Application Programming Interface" (EAPI) used by this module provides a standardized interface for customer applications. This interface allows a user mode application access to hardware specific information as well as hardware resources. Following features are supported:

- view board information
- access to NVRAM
- access to I2C
- control GPIO's
- control backlight
- set watchdog timer
- view sensor values of hardware monitor

MSC provides a software package which is downloadable here after registration

https://embedded.avnet.com/product/msc-c10m-al/#eapi

9 Troubleshooting

Issue 1: USB 3.0 stick causes hang at boot time

Some USB 3.0 sticks/disks may cause BIOS hang at post code 0xB4, if XHCI mapping mode is not set to enabled.

Solution:

Please check for firmware update of the USB device. Alternatively the setting for XHCI mapping mode could be changed to enabled in the BIOS setup.

Issue 2: USB stick recognized as floppy

Some USB sticks are recognized as floppies (show up as "A:" drive under DOS). If this is not wanted, there is a way to handle such an USB stick as a fixed disk (int13h device 8xh).

Solution:

Check in BIOS setup under Advanced -> USB Configuration and at the bottom it should have a list of USB mass storage devices. Here you can choose between Floppy, Forced Floppy, Hard Disk or CD ROM behavior of your USB stick.

Issue 3: SATA 6Gb/s

SATA 6Gb/s behavior is functional only with SATA 6Gb/s cable.

Solution:

Use SATA 6Gb/s cable.

Issue 4: Windows Installation

If Windows Installation setup does not allow to install on harddisk try to make harddisk the first boot device in Bios setup.

Issue 5: Legacy Boot Devices

Because CSM is disabled, only devices with UEFI OS will appear as boot device

For additional help please contact Avnet Embedded /MSC Technical Support:
Phone: +49 - 8165 906-200
Email: support.boards@avnet.eu

```
LICENSE ISSUES OPenSSL
  ======================

  The OpenSSL toolkit stays under a dual license, i.e. both the conditions of
  the OpenSSL License and the original SSLeay license apply to the toolkit.
  See below for the actual license texts. Actually both licenses are BSD-style
  Open Source licenses. In case of any license issues related to OpenSSL
  please contact openssl-core@openssl.org.

  OpenSSL License
  ---------------

/* ====================================================================
 * Copyright (c) 1998-2011 The OpenSSL Project.  All rights reserved.
 *
 * Redistribution and use in source and binary forms, with or without
 * modification, are permitted provided that the following conditions
 * are met:
 *
 * 1. Redistributions of source code must retain the above copyright
 *    notice, this list of conditions and the following disclaimer.
 *
 * 2. Redistributions in binary form must reproduce the above copyright
 *    notice, this list of conditions and the following disclaimer in
 *    the documentation and/or other materials provided with the
 *    distribution.
```

```
*
* 3. All advertising materials mentioning features or use of this
*    software must display the following acknowledgment:
*    "This product includes software developed by the OpenSSL Project
*    for use in the OpenSSL Toolkit. (http://www.openssl.org/)"
*
* 4. The names "OpenSSL Toolkit" and "OpenSSL Project" must not be used to
*    endorse or promote products derived from this software without
*    prior written permission. For written permission, please contact
*    openssl-core@openssl.org.
*
* 5. Products derived from this software may not be called "OpenSSL"
*    nor may "OpenSSL" appear in their names without prior written
*    permission of the OpenSSL Project.
*
* 6. Redistributions of any form whatsoever must retain the following
*    acknowledgment:
*    "This product includes software developed by the OpenSSL Project
*    for use in the OpenSSL Toolkit (http://www.openssl.org/)"
*
* THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT ``AS IS'' AND ANY
* EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE
* IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR
* PURPOSE ARE DISCLAIMED.  IN NO EVENT SHALL THE OpenSSL PROJECT OR
* ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL,
* SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT
* NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES;
* LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)
* HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT,
* STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE)
* ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED
* OF THE POSSIBILITY OF SUCH DAMAGE.
* ====================================================================
*
* This product includes cryptographic software written by Eric Young
* (eay@cryptsoft.com).  This product includes software written by Tim
* Hudson (tjh@cryptsoft.com).
*
*/
```

Original SSLeay License

```
/* Copyright (C) 1995-1998 Eric Young (eay@cryptsoft.com)
 * All rights reserved.
 *
 * This package is an SSL implementation written
 * by Eric Young (eay@cryptsoft.com).
 * The implementation was written so as to conform with Netscapes SSL.
 *
 * This library is free for commercial and non-commercial use as long as
 * the following conditions are aheared to.  The following conditions
 * apply to all code found in this distribution, be it the RC4, RSA,
 * lhash, DES, etc., code; not just the SSL code.  The SSL documentation
 * included with this distribution is covered by the same copyright terms
 * except that the holder is Tim Hudson (tjh@cryptsoft.com).
 *
 * Copyright remains Eric Young's, and as such any Copyright notices in
 * the code are not to be removed.
 * If this package is used in a product, Eric Young should be given attribution
 * as the author of the parts of the library used.
 * This can be in the form of a textual message at program startup or
 * in documentation (online or textual) provided with the package.
 *
 * Redistribution and use in source and binary forms, with or without
 * modification, are permitted provided that the following conditions
 * are met:
 * 1. Redistributions of source code must retain the copyright
 *    notice, this list of conditions and the following disclaimer.
 * 2. Redistributions in binary form must reproduce the above copyright
 *    notice, this list of conditions and the following disclaimer in the
 *    documentation and/or other materials provided with the distribution.
 * 3. All advertising materials mentioning features or use of this software
 *    must display the following acknowledgement:
 *    "This product includes cryptographic software written by
 *     Eric Young (eay@cryptsoft.com)"
 *    The word 'cryptographic' can be left out if the rouines from the library
 *    being used are not cryptographic related :-).
 * 4. If you include any Windows specific code (or a derivative thereof) from
 *    the apps directory (application code) you must include an acknowledgement:
 *    "This product includes software written by Tim Hudson (tjh@cryptsoft.com)"
 *
 * THIS SOFTWARE IS PROVIDED BY ERIC YOUNG ``AS IS'' AND
 * ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE
 * IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE
 * ARE DISCLAIMED.  IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE
 * FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL
 * DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS
 * OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)
 * HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT
 * LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY
 * OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF
 * SUCH DAMAGE.
 *
 * The licence and distribution terms for any publically available version or
 * derivative of this code cannot be changed.  i.e. this code cannot simply be
 * copied and put under another distribution licence
 * [including the GNU Public Licence.]
 */
```

WPA Supplicant License

===

Copyright (c) 2003-2009, Jouni Malinen <j@w1.fi> and contributors
All Rights Reserved.

===

License

This software may be distributed, used, and modified
under the terms of BSD license:

Redistribution and use in source and binary forms, with or without
modification, are permitted provided that the following conditions are
met:

1. Redistributions of source code must retain the above copyright
   notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright
   notice, this list of conditions and the following disclaimer in the
   documentation and/or other materials provided with the distribution.

3. Neither the name(s) of the above-listed copyright holder(s) nor the
   names of its contributors may be used to endorse or promote products
   derived from this software without specific prior written permission.

==============

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT OWNER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

===

Features

Internal crypto implementation (optional):

- X.509 certificate processing in PEM and DER formats
- PKCS #1
- ASN.1
- RSA
- bignum
- minimal size (ca. 50 kB binary, parts of which are already needed for WPA;

TLSv1/X.509/ASN.1/RSA/bignum parts are about 25 kB on x86)

Requirements

----

wpa_supplicant was designed to be portable for different drivers and operating systems. Hopefully, support for more wlan cards and OSes will be added in the future. See developer's documentation (http://hostap.epitest.fi/wpa_supplicant/devel/) for more information about the design of wpa_supplicant and porting to other drivers. One main goal is to add full WPA/WPA2 support to Linux wireless extensions to allow new drivers to be supported without having to implement new driver-specific interface code in wpa_supplicant.

WPA

The original security mechanism of IEEE 802.11 standard was not designed to be strong and has proven to be insufficient for most networks that require some kind of security. Task group I (Security) of IEEE 802.11 working group (http://www.ieee802.org/11/) has worked to address the flaws of the base standard and has in practice completed its work in May 2004. The IEEE 802.11i amendment to the IEEE 802.11 standard was approved in June 2004 and published in July 2004.

Wi-Fi Alliance (http://www.wi-fi.org/) used a draft version of the IEEE 802.11i work (draft 3.0) to define a subset of the security enhancements that can be implemented with existing wlan hardware. This is called Wi-Fi Protected Access<TM> (WPA). This has now become a mandatory component of interoperability testing and certification done by Wi-Fi Alliance. Wi-Fi provides information about WPA at its web site (http://www.wi-fi.org/OpenSection/protected_access.asp).

IEEE 802.11 standard defined wired equivalent privacy (WEP) algorithm for protecting wireless networks. WEP uses RC4 with 40-bit keys, 24-bit initialization vector (IV), and CRC32 to protect against packet forgery. All these choices have proven to be insufficient: key space is too small against current attacks, RC4 key scheduling is insufficient (beginning of the pseudorandom stream should be skipped), IV space is too small and IV reuse makes attacks easier, there is no replay protection, and non-keyed authentication does not protect against bit flipping packet data.